НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
Факультет інформатики та обчислювальної техніки
Кафедра технічної кібернетики

«На правах рукопису»
УДК 004.056

До захисту допущено:
Завідувач кафедри
_____ Ігор ПАРХОМЕЙ
«___»_____2020 р.

Магістерська дисертація

на здобуття ступеня магістра

за освітньо-професійною програмою «Інформаційне забезпечення робототехнічних систем»

зі спеціальності 126 «Інформаційні системи та технології»

на тему: «Система моніторингу та оцінки загроз інформаційній безпеці розумного будинку»

Виконав:
студент ІІ курсу, групи ІК-91мп
Донченко Андрій Григорович _____

Керівник:
доцент, к.т.н.,
Цьопа Наталія Володимирівна _____

Консультант з нормоконтролю:
доцент, к.т.н., доц.,
Пасько Віктор Петрович _____

Рецензент:
професор КБЗІ КНУ ім. Т.Шевченка
д.т.н., професор
Толюпа Сергій Васильович _____

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____

Київ – 2020 року

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Факультет інформатики та обчислювальної техніки

Кафедра технічної кібернетики

Рівень вищої освіти – другий (магістерський)

Спеціальність – 126 «Інформаційні системи та технології»

Освітньо-професійна програма «Інформаційне забезпечення робототехнічних систем»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Ігор ПАРХОМЕЙ

«___»_____2020 р.

ЗАВДАННЯ
на магістерську дисертацію студенту

Донченкові Андрієві Григоровичу

1. Тема дисертації «Система моніторингу та оцінки загроз інформаційній безпеці розумного будинку», науковий керівник дисертації Цьопа Наталія Володимирівна доцент, к.т.н., затверджені наказом по університету від «26» жовтня 2020р. № 3132-с

2. Термін подання студентом дисертації _____23.11.2020 р._____

3. Об’єкт дослідження – система «розумний будинок» і виникаючі в ній загрози інформаційній безпеці.

4. Вихідні дані – програмний продукт повинен мати можливість налаштування складу системи «розумний будинок», виконувати моніторинг стану системи «розумний будинок» та оцінку виникаючих загроз інформаційній безпеці.

5. Перелік завдань, які потрібно розробити – аналітичний огляд предметної області; огляд і порівняння існуючих рішень; розробка класифікації загроз інформаційній безпеці; проектування інформаційної системи моніторингу та оцінки загроз інформаційній безпеці технології «розумний будинок»; розробка прототипу інформаційної системи моніторингу та оцінки загроз інформаційній безпеці технології «розумний будинок»

6. Орієнтовний перелік графічного (ілюстративного) матеріалу – шість плакатів.

7. Орієнтовний перелік публікацій – 1 публікація.

8. Консультанти розділів дисертації

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Перевірка на співпадіння	доцент Лісовиченко О.І.		
Нормоконтроль	доцент Пасько В.П.		

9. Дата видачі завдання 27.09.2019 р.

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Огляд технології «розумний будинок»	01.09.2020 – 08.09.2020	
2	Аналіз предметної області	08.09.2020 – 17.09.2020	
3	Класифікація загроз інформаційній безпеці	18.09.2020 – 27.09.2020	
4	Проектування системи інформаційної безпеки	28.09.2020 – 15.10.2020	
5	Розробка програмного забезпечення	16.10.2020 – 03.11.2020	
6	Маркетинговий аналіз стартап-проєкту	4.11.2020 – 18.11.2020	
7	Попередній захист	23.11.2020	
8	Нормоконтроль		
9	Перевірка на співпадіння		
10	Захист		

Студент Андрій ДОНЧЕНКО

Науковий керівник Наталія ЦЬОПА

АНОТАЦІЯ

У роботі розглянуто проблеми в області інформаційної безпеки у системах розумного будинку. Приведено основні особливості існуючих рішень, наведені їх переваги та недоліки.

Запропоновано класифікацію ймовірних загроз інформаційній безпеці систем розумного будинку, що зв'язує можливі загрози з об'єктами керування.

В результаті дослідження спроектовано систему моніторингу і оцінки загроз для розумного будинку і розроблено програмний додаток для спроектованої системи.

Основними функціями системи є визначення складу системи розумного будинку і установка обмежень для показань об'єктів керування користувачем або автоматично, моніторинг даних і генерація оповіщень про стан системи розумного будинку. Розроблена система може бути використана в житлових приміщеннях, в яких встановлена система «розумний будинок».

Ключові слова: розумний будинок, інформаційна безпека, загрози інформаційній безпеці.

Розмір пояснювальної записки – 80 аркушів, містить 23 ілюстрації, 25 таблиць, 7 додатків.

ABSTRACT

The paper considers the problems in the field of information security in smart home systems. The main features of existing solutions, their advantages and disadvantages are given.

The classification of probable threats to information security of smart home systems is proposed, which connects possible threats with control objects.

As a result of the research, a system for monitoring and threat assessment for a smart home was designed and a software application for the designed system was developed.

The main functions of the system: determining the composition of the smart home system and setting limits on the readings of controlled objects by the user or automatically, data monitoring and generation of alerts about the status of the smart home system. The developed system can be used in living quarters in which the "smart home" system is installed.

Key words: smart home, information security, information security threats.

The size of the explanatory note is 80 sheets, contains 23 illustrations, 25 tables, 7 appendices.

Пояснювальна записка

до магістерської дисертації

на тему: ***Система моніторингу та оцінки загроз інформаційній безпеці розумного будинку***

Київ – 2020 року

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

РБ – розумний будинок;

ІБ – інформаційна безпека;

БД – база даних;

ПЗ – програмне забезпечення;

IoT (Internet of things) – інтернет речей;

UML (unified modeling language) – уніфікована мова моделювання;

XML (extensible markup language) – розширювана мова розмітки;

XML Schema – мова опису структури XML-документу.

ВСТУП

Система "розумний будинок" є апаратно-програмним комплексом, всередині якого обробляється великий потік інформації, в зв'язку з чим вона є схильною до загроз інформаційній безпеці. На жаль, сучасні розробки в області технології розумного будинку не містять єдиної методології опису систем РБ, тому відсутня і єдина методологія виявлення і оцінки загроз інформаційній безпеці технології "розумний будинок".

Загрози інформаційної безпеки залежать від методів побудови системи РБ, застосовуваних технологій і оброблюваної інформації, що підтверджують автори статті [5], представленої на Міжнародному симпозіумі "Надійність і якість". Тестування декількох загальнодоступних систем розумного будинку, проведене компанією AV-TEST [2], доводить наявність проблем з інформаційною безпекою в пропонованих компаніями системах РБ. Багато існуючих рішень для додаткового захисту інформаційної безпеки розумного будинку використовують метод роботи, що полягає в підключенні до роутера і моніторингу потоку інформації між підключеними до Wi-Fi пристроями. Даний метод обмежує коло підтримуваних пристроїв. Також деякі з існуючих рішень здійснюють додатковий збір і відправку даних про роботу пристроїв розумного будинку в хмарне сховище, що може стати додатковою загрозою.

Наведені аспекти аналізу стану галузі інформаційної безпеки технології РБ доводять актуальність обраної теми.

РОЗДІЛ 1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ І ПОСТАНОВКА ЗАДАЧІ

1.1. Технологія "розумний будинок"

Під терміном "розумний будинок" (РБ) прийнято розуміти сукупність підключених до загальної мережі пристроїв, що виконують певні дії з мінімальним втручанням з боку людини. Ідея створення РБ в наближеному до сьогоднішнього розуміння цього терміну з'явилася в кінці 20 століття. Один з перших таких будинків був описаний в журналі "Popular Mechanics" в 1950 році. Термін "розумний будинок" був введений в 1984 році американською Асоціацією житлово-будівельних компаній і до 2000 року ідея "розумних будинків" була досить поширена в Європі і, особливо, в США.

Технологія РБ використовується для різних цілей, можна виділити основні з них :

- тепло та енергозбереження;
- підвищення комфорту;
- забезпечення безпеки.

Різні підприємства застосовують технологію РБ в основному для енергозбереження та безпеки, в житлових приміщеннях системи розумного будинку можуть використовуватися для всіх вищезазначених цілей.

Компанії виробники систем розумного будинку пропонують різні варіації систем: готові рішення "під ключ" і системи, які налаштовуються під вимоги конкретного клієнта. Також на ринку представлені окремі "розумні" продукти (в основному випускаються виробниками техніки), які користувач може самостійно об'єднати в систему РБ.

Системи "розумний будинок" не мають єдиної методології опису. Як компанії, так і дослідники технології РБ, мають різні підходи до опису системи розумного будинку. Найбільш частіше зустрічається підхід – поділ системи РБ на різні підсистеми. Узагальнений опис видів підсистем розумного будинку представлено на рис. 1.1.

Рис. 1.1. Підсистеми розумного будинку

1.2. Об'єкт та предмет дослідження

Об'єкт дослідження: системи "розумний будинок" і виникаючі в них загрози інформаційній безпеці. Так як загрози інформаційній безпеці залежать від методів побудови системи, використовуваних технологій і оброблюваних інформаційних потоків, досліджувані системи розумного будинку були звужені до систем "розумний будинок", що застосовуються в житлових будинках.

Предмет дослідження: методи проектування системи інформаційної безпеки технології "розумний будинок".

1.3. Захист інформаційної безпеки у розумному будинку

Система розумного будинку є об'єктом інформатизації, схильним до загроз інформаційній безпеці. Загрози інформаційній безпеці системи залежать від методів побудови системи, використовуваних технологій і оброблюваних інформаційних потоків, тому не існує єдиної методології способу захисту інформаційної безпеки.

Багато систем розумного будинку мають вбудований компонент захисту інформаційної безпеки, але, на жаль, даний компонент не завжди гарантує високий рівень захисту. У деяких системах компонент інформаційної безпеки може навіть бути відсутнім. З цієї причини деякі компанії почали виробництво додаткових засобів

захисту інформаційної безпеки розумного будинку, але, якщо компанія є виробником "розумних" пристроїв, то в більшості випадків засіб захисту, який розроблюється, здатен працювати тільки з "розумними пристроями" цієї компанії.

У 2014 році компанія AV-TEST, що є незалежним інститутом інформаційної безпеки, провела тестування декількох загальнодоступних систем РБ. AV-TEST досліджувала:

- наявність шифрованого зв'язку між елементами РБ;
- використання активної аутентифікації;
- можливість зовнішньої маніпуляції;
- рівень захищеності віддаленого доступу.

Результати тестування семи систем РБ показали:

- лише три системи забезпечують інформаційну безпеку;
- дві системи недостатньо захищені і можуть бути схильні до внутрішніх атак;
- дві системи мають дуже слабкий інформаційний захист і можуть бути схильні як до внутрішніх, так і до зовнішніх атак.

Проведене тестування доводить, що навіть користувачам готових рішень не слід забувати про інформаційний захист і при необхідності використовувати додаткові засоби захисту, а виробникам РБ потрібно випускати продукти з більш високим рівнем захисту.

1.4. Існуючі рішення захисту інформації систем "розумний будинок"

Як було сказано раніше, компанії-виробники засобів захисту інформації для РБ, які одночасно є виробниками "розумних" пристроїв, найчастіше розробляють засоби захисту для своїх пристроїв. Але інші компанії роблять універсальні засоби захисту інформації. Далі розглянуті кілька прикладів таких пристроїв.

Один з поширених методів роботи на ринку пристроїв додаткового інформаційного захисту РБ – підключення до роутера і моніторинг потоку інформації між підключеними до Wi-Fi пристроями.

Три яскраві приклади подібних пристроїв:

- Dojo, розроблене невеликою ізраїльською компанією Dojo-Labs;
- CUJO, розроблене групою каліфорнійських дослідників;
- Bitdefender Box, вироблене великою компанією Bitdefender.

Основний недолік даних пристроїв обумовлений вибором методу роботи, що обмежує захищувані пристрої. Крім цього, пристрої Dojo і CUJO здійснюють додатковий збір і відправлення в "хмару" даних про роботу пристроїв, для визначення нових загроз. Додатковий збір даних може бути додатковою загрозою інформаційній безпеці, так як віддалена "хмара" може бути так само схильна до атак хакерів.

Існують і більш функціональні засоби захисту інформаційної безпеки, які можуть контролювати всю мережу РБ і не збирати додаткові дані. Приклад подібних пристроїв - серія пристроїв Cisco ASA 5500-X с функціями FirePOWER, вироблена однією з найбільших IT-компаній Cisco. Але запропоновані функціональність і якість мають відповідну ціну і складність установки та експлуатації, так як подібні пристрої розроблені в основному для використання в середніх і великих компаніях, які мають необхідний персонал або можливість використання досить дорогого сервісного обслуговування.

1.4.1. Dojo

Dojo – це пристрій захисту інформації, розроблений невеликою ізраїльською компанією "Dojo-Labs". Компанія націлена на створення зручного для споживача інтерфейсу безпеки та управління на мережевому рівні, який здатний виявляти та блокувати аномальну поведінку підключених пристроїв у домашній мережі.

Біла коробка Dojo підключається до маршрутизатора Wi-Fi і відстежує весь мережевий трафік в режимі реального часу та виявляє аномалії та загрози. "Digital pet rock" має систему світлодіодів, що вказують на стан безпеки. Це єдина функція цього компонента, крім дизайну. Управління Dojo здійснюється за допомогою додатку для смартфону "Dojo App". Усі сповіщення з’являються у програмі, яка дозволяє

користувачеві знати про проблеми, перш ніж вони вплинуть на його конфіденційність або безпеку (рис. 1.2).

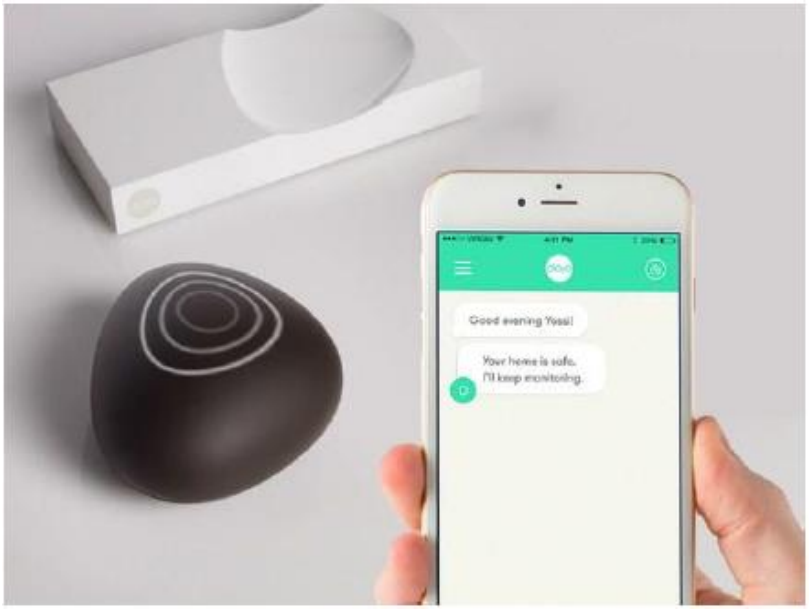


Рис. 1.2. Компоненти Dojo

Dojo підключений до хмарного сховища даних, щоб вивчати метадані з пристроїв користувача та покращувати виявлення загроз. Це розумне рішення для збільшення відомої бази даних загроз, але воно також представляє великий інтерес для хакерів. "Один хмарний сервер з величезною кількістю метаданих" - звучить досить привабливо. Іншим недоліком є відсутність взаємодії з не підключеними до Інтернету пристроями, на які також можуть впливати загрози.

1.4.2. CUJO

CUJO – це пристрій захисту інформації, розроблений групою каліфорнійських дослідників. Засновники проекту отримали фінансування на веб-сайті краудфандингу.

Для захисту пристроїв від широкого спектру атак CUJO використовує багатошаровий підхід, що поєднує в собі як брандмауер, так і антивірус. Він діє як шлюз між пристроями та для підключення до Інтернету. CUJO дуже схожий на Dojo. Справа не лише в іменах. CUJO має привабливий дизайн з "очима" - індикаторами. Як і Dojo, пристрій підключається до маршрутизатора Wi-Fi і контролює трафік. CUJO

управляється смартфоном і також використовує хмару (рис. 1.3). Пристрій має ті ж недоліки, що і CUJO.

Рис. 1.3. Вигляд CUJO

1.4.3. Bitdefender Box

Bitdefender Box розроблена великою румунською компанією Bitdefender, що спеціалізується на антивірусних продуктах (рис. 1.4). На офіційному веб-сайті є три варіанти продуктів для різних рівнів захисту та ряду підключених пристроїв. На жаль, Bitdefender Box сертифікований для використання лише в США, Франції та Японії. Ось чому цей пристрій наразі доступний лише в цих країнах.

Рис. 1.4. Вигляд Bitdefender Box

Bitdefender BOX постійно сканує, виявляє та висвітлює недоліки мережевої безпеки. Він шукає приховані бекдори та погано захищені порти управління.

Продукт працює як два попередні пристрої: коробчастий пристрій, модем, додаток для смартфона та хмарне сховище даних. У нього все ті ж недоліки. Спеціалізація компанії та великий досвід дозволили не збирати надлишкові дані. Це виявляється головною перевагою Bitdefender Box.

1.4.4. Cisco ASA 5500-X

Cisco ASA 5500-X - with FirePOWER Services (рис. 1.5) – це серія пристроїв із інтегрованими брандмауерами, орієнтованими на загрози, виробленими величезною багатонаціональною американською компанією "Cisco Systems, Inc. " (Cisco). Cisco спеціалізується на Інтернеті речей, безпеці доменів та управлінні енергетикою. Cisco розробляє та виробляє мережеве обладнання, телекомунікаційне обладнання та інші продукти. Серед основних споживачів є великі та малі підприємства.

Рис. 1.5. Вигляд Cisco ASA 5500-X - with FirePOWER Services

Ці пристрої є брандмауерами з розширеною функцією моніторингу з'єднань, що забезпечує прозорість та обізнаність у контексті програми. Серія має простий дизайн, що є типовим для таких пристроїв.

Головною перевагою цієї серії є висока ефективність захисту інформації, підтверджена тестами. Це високотехнологічний продукт із відповідною ціною. Серія

розроблена для малих та великих підприємств і вимагає досить складних монтажу та обслуговування та, як наслідок, висококваліфікованого персоналу.

1.4.4. Основні недоліки існуючих рішень-конкурентів

Слабкими сторонами конкурентів є:

- конкурент 4 поступається в зручності експлуатації, так як продукт в основному розрахований для використання на підприємствах, де співробітники, які безпосередньо взаємодіють з продуктом, зазвичай спочатку проходять інструктаж або навчання роботі з даним продуктом;
- у конкурентів 1-3 існує можливість лише мінімальної настройки роботи продукту;
- конкуренти 1-3 поступаються в функціональної потужності, їх продукти можуть працювати тільки з приладами, що використовують інтернет-з'єднання;
- конкуренти 1-2 використовують додатковий збір і відправку даних про роботу своїх продуктів;

1.5. Постановка задачі

Мета роботи - проектування системи моніторингу та оцінки загроз інформаційній безпеці технології "розумний будинок" і розробка програмного додатку спроектованої системи.

Для досягнення мети необхідно вирішити наступні задачі:

1. визначити типи задач, виконувані системою та проаналізувати їх методи вирішення;
2. спроектувати систему класифікації загроз інформаційній безпеці розумного будинку;
3. реалізувати додаток для розроблюваної системи.

Створений продукт повинен відповідати таким вимогам:

- система повинна визначати склад системи розумного будинку, проводити моніторинг даних та генерувати сповіщення про знайдені загрози;

- зручність у використанні;
- простота у налагодженні;
- можливість застосовувати даний продукт для будь-якої системи розумного будинку.

Висновки по розділу 1

У даному розділі описано термін, коротку історію виникнення та застосування розумного будинку, наведені його основні підсистеми. Проведено аналіз предметної області, визначені об’єкт та предмет дослідження, розглянута система розумного будинку у контексті захисту інформаційної безпеки.

Наведено результати тестування різних систем розумного будинку компанією AV-TEST, які показали, що більша частина систем захищена недостатньо, або є зовсім незахищеною від атак хакерів.

Проведено огляд існуючих рішень, описано принципи роботи даних рішень та визначені їх недоліки. В результаті проведеного аналізу сформульована мета роботи, поставлені задачі та вимоги для розроблюваної системи.

РОЗДІЛ 2. АНАЛІЗ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ

2.1. Модель побудови системи моніторингу інформаційної безпеки

Відсутність єдиної методології побудови захисту інформаційної безпеки технології розумного будинку пояснює різні структури і методи роботи засобів захисту. Розробку цих засобів можна умовно розділити на наступні етапи:

- опис моделі системи розумного будинку;
- опис моделі загроз інформаційній безпеці;
- розробка методів оцінки загроз;
- розробка автоматичного механізму моніторингу стану захисту розумного будинку.

Методи оцінки загроз ґрунтуються на моделі системи РБ і моделі загроз, можуть використовувати список найбільш ймовірних загроз і критерії: джерела загроз, вразливості, можливі наслідки та ін.

Один із прикладів списку найбільш ймовірних загроз містить такі загрози:

- хакерські атаки на центральний сервер;
- вплив вірусних і троянських програм на роботу системи;
- перехоплення інформації, що передається по дротовим і бездротовим каналам зв'язку;
- доступ зловмисника з правами адміністратора на центральний сервер за допомогою розкрадання паролів і інших реквізитів розмежування доступу;
- доступ до мережі неавторизованих користувачів;
- наявність порушників серед обслуговуючого персоналу;
- помилки користувача;
- зловмисне виведення з ладу апаратури;
- перебої в мережі електроживлення;
- стихійні лиха;
- поломка апаратури системи;
- помилки програмного забезпечення;

– витік інформації через побічні електромагнітні випромінювання і наводки;
– витік інформації по акустоелектричному каналу.

Модель проектованої системи:

– опис моделі системи розумного будинку;
– опис моделі загроз інформаційній безпеці;
– розробка методів оцінки загроз;
– розробка автоматичного механізму моніторингу стану захисту розумного будинку.

Для проектування системи інформаційної безпеки використовуються основні методи системного аналізу і технології розробки програмного забезпечення. Системний аналіз застосовується для вирішення важко формалізованих і слабко структурованих проблем для приведення складної проблеми до взаємозалежної ієрархії більш простих завдань.

В результаті аналітичного огляду предметної області було прийнято рішення використовувати спосіб опису системи "розумний будинок" шляхом поділу системи на підсистеми, тому що даний спосіб використовується багатьма дослідниками і виробниками систем РБ. В системі "розумний будинок" були виділені наступні підсистеми:

– підсистема керування і зв'язку;
– підсистема безпеки і моніторингу;
– підсистема електроживлення;
– підсистема освітлення;
– підсистема опалення;
– підсистема вентиляції;
– підсистема кондиціонування;
– підсистема мультимедіа.

Далі пропонується розбиття підсистем на компоненти, об'єкти керування і елементи: датчик і виконавчий механізм. Компоненти відповідають за роботу з об'єктами керування, а у об'єкта керування повинен бути зазначений тип підсистеми.

Всі об'єкти керування в розумному будинку мають датчик для зчитування необхідних даних і виконавчий механізм, що виконує будь-яку дію. Показник датчика і дія виконавчого механізму безпосередньо впливають на стан об'єкта і стан інформаційної безпеки всієї системи РБ, тому для них повинні визначатися обмеження.

Отримання даних про склад системи РБ передбачається наступними способами:

1. Користувач самостійно описує кожен елемент системи РБ.

2. Система інформаційної безпеки автоматично збирає дані з системи РБ і визначає на їх основі склад системи РБ.

Для побудови класифікації загроз інформаційній безпеці технології РБ було вирішено використовувати список найбільш ймовірних загроз, описаний в попередньому розділі і використовувати такі критерії:

- величина відхилення значення датчика або виконавчого механізму;
- можливі джерела загрози;
- можливі наслідки загрози;
- вразливості.

Список загроз визначається для різних об'єктів управління в залежності від підсистем, в яких вони розташовуються, та в залежності від ступеня відхилення даних датчика або виконавчого механізму.

Метод моніторингу стану РБ ґрунтується на наступних етапах:

- опис системи РБ користувача;
- отримання даних з системи РБ;
- аналіз даних, порівняння з встановленими обмеженнями;
- визначення підсистеми і об'єкта, в якому виникла загроза;
- оцінка загрози за визначеним списком загроз.

Для опису моделі системи РБ і загроз в проектованій системі обрана мова XML, для опису структури даних файлів обрана мова XML-Schema. Вибір мов опису даних обумовлений великою вкладеністю і великим обсягом даних, формат XML ефективний в роботі саме з такими даними. XML це розширювана мова розмітки, яка дозволяє створити будь-яку необхідну для конкретної області застосування розмітку. Структуру

XML-файла можна описати за допомогою специфікації XML-Schema, яка визначає правила документа. XML має реалізації "парсерів" (програми для аналізу розмітки) для всіх сучасних мов програмування. Також XML підтримується на низькому апаратному, мікропрограмному і програмному рівнях в сучасних апаратних рішеннях.

Для розробки прототипу спроектованої системи обрані:

- середовище розробки Microsoft Visual Studio 2019;
- мова програмування C #;
- система для побудови клієнтської програми Windows Presentation Foundation (WPF).

2.2. Основні бездротові протоколи передачі даних у розумному будинку та їх вразливості

1) Bluetooth. це бездротовий протокол для короткого діапазону (максимум до 100 метрів) підключення. Bluetooth є відносно надійний, та не потребує високої потужності для роботи. Він використовує схему дуплексу з поділом часу для повної дуплексної передачі даних. Іншими словами, Технологія Bluetooth просто використовує низьку потужність радіохвилі для підключення електронного пристрою до іншого без фізичного зв’язку. Bluetooth призначений бути стандартом, який діє на двох рівнях: Це забезпечує узгодження на фізичному рівні для ідентифікації пристроїв та передача даних. Він також забезпечує узгодження на одному рівні вище, наприклад синхронізація пристроїв, обмеження передачі даних між часовими рамками та методологією для сторін які передають дані, за допомогою якої можна переконатися, що отримане повідомлення повністю відповідає надісланому повідомленню.

2) ZigBee. ZigBee, подібно до Bluetooth, має велику встановлену база операцій, вона має два варіанти, ZigBee PRO і ZigBee Remote Control (RF4CE), обидва базуються на протоколі IEEE802.15.4, який працює на пропускній здатності 2,4 ГГц, яка потребує потрібно порівняно рідкі обміни даними з низькою швидкістю передачі даних на обмеженій території та в межах 100 м, таких як дім або будівля. ZigBee має деякі переваги, такі як низьке споживання енергії, відносно висока безпека, висока

масштабованість і надійність при великій кількості вузлів у бездротовій сенсорній мережі для машинного зв’язку та додатків IoT. Його нещодавня версія ZigBee 3.0 має діапазон 10-100 м та швидкість передачі даних 250 кбіт / с.

3) Z-Wave. це комунікаційна технологія на радіочастотах малої потужності, яка спеціально розроблена для пристроїв домашньої автоматики, таких як контролери ламп, розумні контролери світла та датчики серед багатьох інших пристрої. Він оптимізований для надійного зв’язку з низькими затримками для передачі малих пакетів даних зі швидкістю передачі даних до 100 кбіт / с. Він працює на частоті 900 МГц (ISM) з радіусом дії 30 метрів. На цій частоті Z-Wave не інтерферує з бездротовими протоколами, які працюють на частоті 2,4 ГГц, такими як WiFi та інших бездротових протоколів у діапазон 2,4 ГГц, такий як ZigBee або Bluetooth. Він може підключитися до 232 пристроїв і підтримує повнозв'язні мережі і не потребує вузол координатора, є дуже масштабованим. Z-Wave використовує простіший протокол, ніж деякі інші, що дозволяє швидше і простіше розроблювати програму, але це лише підтримує чіпи Sigma Designs у порівнянні з багатьма джерелами для інших бездротових технологій, таких як BLE, ZigBee, Sigfox та інших.

4) 6LoWPA. Це відкритий стандарт, визначений у RFC 6282 Робочою групової інженерів Інтернету (IETF) - організацією по стандартизації, яка визначає безліч відкритих стандартів, що використовуються в Інтернеті, такі як UDP, TCP та HTTP. Чудова особливість 6LoWPAN включається в тому, що він був в першу чергу задуманий для підтримки малопотужних безпровідних мереж 2,4 ГГц, побудованих на базі IEEE 802.15.4, тепер цей стандарт адаптований і використовується в багатьох інших середовищах мережевих передачах, включаючи безпровідні мережі в діапазонах нижче 1 ГГц, Smart Bluetooth, передачу даних по лінії електропередач (PLC) і малопотужні мережі Wi-Fi.

5) Thread. Нова мережа на базі IPv6 протоколу, розроблена спеціально для домашньої автоматизації. Він заснований на 6LowPAN і є не протоколом для інтернету речей на відміну від, наприклад, ZigBee, BLE, Z-Wave, Bluetooth, оскільки він в основному був розроблений як доповнення до WiFi, але може бути застосований для

встановлення домашньої мережі з деякими обмеженнями для сетапу домашньої автоматизації. Він був випущений в середині 2014 року компанією Thread Group, протокол базується на наборі стандартів, включаючи IPv6, 6LoWPAN та IEEE802.15.4 і здатний налаштувати мережу на основі IP для пристроїв з підтримкою IoT. Він підтримує сітчасту мережу з 250 вузлами з діапазоном до 30 метр зі швидкістю передачі даних до 250 кбіт / с на радіо частотах 2,4 ГГц (ISM).

6) WiFi. Технологія WiFi зазвичай використовується в будинків та офісах, що використовують стандарт IEEE802.11n і забезпечує високу швидкість передачі даних до 1 Гбіт / с (залежно від частоти каналу 2,4 ГГц або 5 ГГц) в діапазоні 50 метрів. Існує широка інфраструктура, яка використовує WiFi як протокол зв'язку для швидкої передачі даних та обробки великої кількості даних. Він також забезпечує інтерпретацію з Ethernet, IP-мережами, такими як 6LowPan і Thread, але це вимагає більше енергії, і може бути вибором розробників для розумної автоматизація будинку.

7) Celluar (Стільниковий). Будь-який IoT додаток, який працює і управляє на великій відстані може використовувати протокол стільникового зв'язку GSM / 3G / 4G / LTE для передачі та обміну даними. Стільникова технологія має можливість надсилати і отримувати велику кількість даних на швидкості 35-170 к / с (GPRS), 120-384kbps (EDGE), 384Kbps-2Mbps (UMTS), 600 кбіт / с - 10 Мбіт / с (HSPA), 3-10 Мбіт / с (LTE) та 20+ Мбіт / с (4G). Особливо для 4G, витрати, а також споживання енергії у багатьох випадках можуть бути високими, але такий підхід може бути ідеальним для проекту з низькою пропускною здатністю на основі датчиків що передають низькі обсяги інформації або даних через інтернет.

8) SigFox. Це альтернативна широко-діапазонна комунікаційна технологія, що використовуються допоміжними пристроями Інтернету речей. Для передачі даних SigFox використовує ультра-вузьку смугу частот (Ultra- Narrow Band, UNB) з двійково-фазової маніпуляцією (BPSK), а для кодування даних змінює фазу несучої радіохвилі. Це дозволяє зменшити рівень шуму на приймаючій стороні, отже, зробити приймаючі пристрої більш дешевими. Радіус дії: 30-50 км (3-10 км в зашумлених і важкодоступних районах). Термін служби пристроїв які використовують SigFox без

заміни батареї склада близько 20 років від 2-х батарейок типу АА. Використовувані частоти: 868 МГц (Європа) і 902 МГц (США). Топологія мережі: зірка (базова станція, до якої підключаються кінцеві точки).Існуючий стандарт SigFox визначає максимальну кількість повідомлень від базової станції до кінцевого пристрою в день: 140 повідомлень, при цьому кожне повідомлення має бути розміром не більше 12 байт (виключаючи заголовок повідомлення та інформацію про передачу). І також кількість повідомлень, що виходять від кінцевого пристрою: 4 повідомлення в день з корисним навантаженням 8 байт.

9) LoRaWAN (Long range wide area network) – це MAC протокол для високоємких мереж з великим радіусом дії і низьким власним споживанням потужності. У деякому плані він схожий на Sigfox. Типовий діапазон становить 5 км (міське середовище) і 15 км (заміська середа). Дана технологія розроблена і призначена реалізувати малопотужні широкозонні мережі для підтримки мобільного захищеного двостороннього зв'язку в машинній взаємодії, інтернеті речей, розумному місті, розумному будинку і інших промислових застосуваннях. LoRaWAN забезпечує повний двосторонній зв’язок, а спеціальні методи шифрування – загальну надійність та безпеку. Дану технологію оптимізовано для малопотужного споживання зі швидкістю передачі даних від 0,3 Кбіт/с до 50 Кбіт/с, а також підтримує великі мережі з мільйонами різноманітних приладів та пристроїв.

2.2.1. Проблеми безпеки, загрози та вразливості протоколів передачі даних

У табл. 2.1 наведені основні вразливості бездротових протоколів передачі даних.

Таблиця 2.1. Перелік уразливостей протоколів передачі даних

№	**Назва протоколу**	**Основні проблеми/вразливості/фактори, які є загрозами інформаційній безпеці**
1	Bluetooth	• Bluejacking (атака bluetooth-спамом); • Bluebugging (несанкціонована передача даних хакерами); • Bluesnarfing (доступ до хакерів файлів за допомогою Bluetooth приєднання).

Таблиця 2.1. (закінчення)

2	ZigBee	• Фізичні атаки; • Атаки на зв’язаних ключах; • Атаки повторного підтворення; • Ін’єкційні атаки (Injection attacks).
3	Z-Wave	• Спурфінг атаки • Виявлення зовнішньої топології • Довільна модифікація SR кешу • Атаки відбрасування пакетів
4	6LowPan	• Обмеження безпеки транспортного рівня • Проблеми безпеки з захистом транспортного рівня • Не підтримує неаппельованість • Не забезпечує поетапний відпис та шифрування
5	WiFi	• WEP та Wi-Fi захищений доступ (WPA) можливо взламати за хвилини • WPA2 також може бути взламаний, але якщо користувач налаштує його належним чином, це займе більше часу у злочинця • Дуже легко прослуховується.
6	Celluar	• Відстеження місцезнаходження • Викрадення смуги пропускання • Проблеми безпеки через відкриту архітектуру • DoS атаки
7	Thread	• Всі вразливості від протоколу 6LowPan • Служби UDP серйозно впливають на уразливості системи безпеки.
8	SigFox	• Проблема безпеки даних на мережевому рівні • Обмежене застосування • Менший обсяг даних
9	LoRaWAN (Long Range wide Area Network)	• Неоптимальні методи шифрування • Проблеми, пов’язані з ключами шифрування • Проблеми з довірою при обробці даних на передавальних пристроях. • Проблема з взломуванням шлюзу • Компоненти взламаного доступу в Інтернету є частою метою для хакерів.

2.3. Класифікація джерел загроз ІБ

Джерелами виступають суб’єкти так і об’єктивні прояви. При цьому джерела загроз розділимо на дві категорії: внутрішні джерела, тобто ті, які перебувають всередині організації, яка є захищуваною та зовнішні, тобто ті, які перебувають поза захищуваною організацією. На рис. 2.1 наведено класифікацію загроз безпеці інформації на загрози: доступності, цілісності та конфіденційності.

Рис. 2.1. Класифікація загроз безпеці інформації

Проаналізувавши всі існуючі джерела загроз інформаційній безпеці (ІБ) поділимо їх на 3 основні групи (рис. 2.2):

I. Антропогенні або суб'єктивні.

II. Техногенні.

III. Стихійні (або природні) джерела.

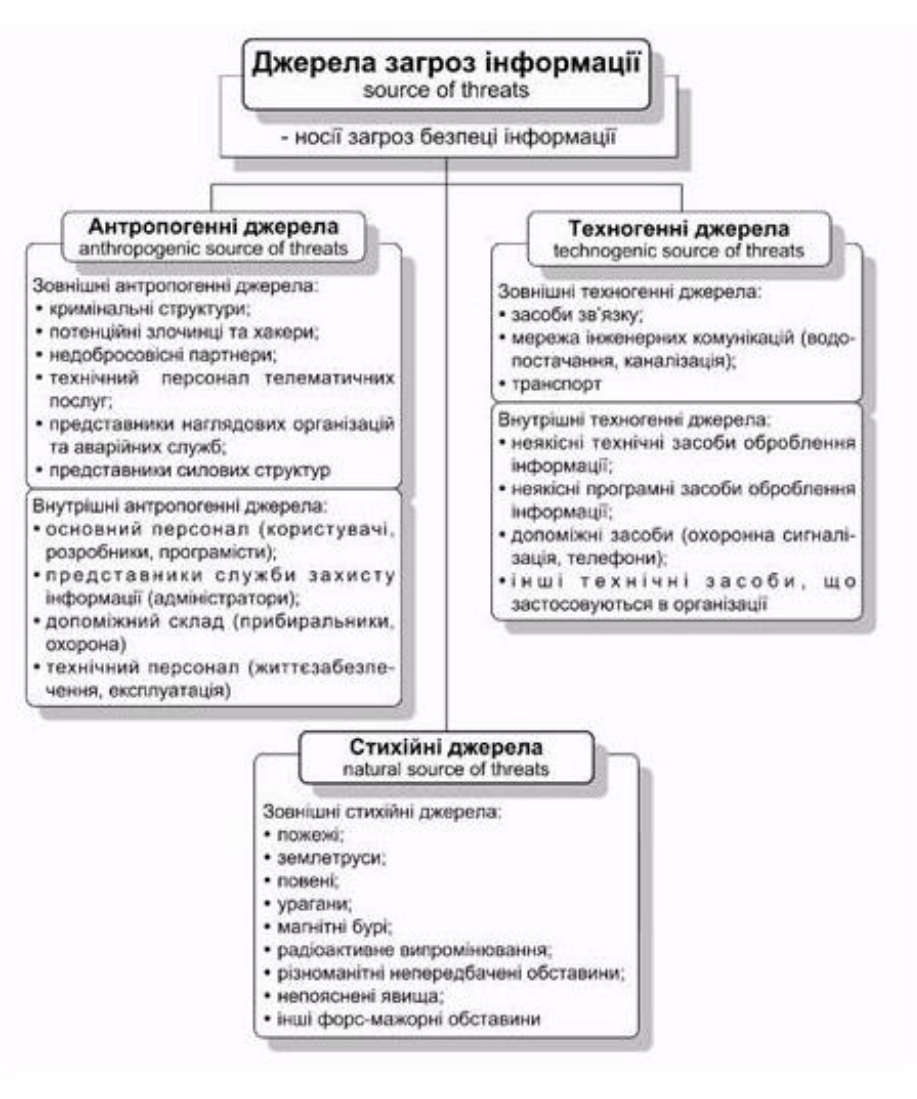


Рис. 2.2. Класифікація джерел загроз інформації

2.3.1. Антропогенні джерела загроз ІБ

Суб'єктивними(або антропогенними) джерелами небезпек є суб’єкти (люди), дії яких можна визначити як умисні або неумисні злочини. Ця група є найбільшою за розмірами, порівняно з іншими, і представляє високий інтерес з точки зору того як найбільш вдало організувати інформаційну безпеку, оскільки дії суб’єкта, як правило, можна оцінити, передбачити та вжити необхідних заходів. Методика протидії суб’єктам в цьому випадку визначається організаторами.

Суб’єкт, який має доступ (уповноважений чи неуповноважений) для роботи зі стандартними засобами об’єкта, що охороняється, може розглядатися як антропогенне

джерело загроз. Суб'єкти, дії яких призводять до порушень інформаційної безпеки, поділяють на два типи: зовнішні [I.A.], так внутрішні [I.B.].

Зовнішні джерела загроз ІБ бувають випадковими та невипадковими та крім цього мають певний рівень кваліфікації. До таких належать:

- [I.A.1] злочинні структури;
- [I.A.2] можливі злочинці та хакери;
- [I.A.3] нечесні партнери;
- [I.A.4] інженерно-технічний персонал який постачає інформаційні послуги;
- [I.A.5] інженерно-персонал організацій спостереження;
- [I.A.6] правоохоронні органи та силові структури.

Внутрішні суб'єкти є висококваліфікованими спеціалістами у галузі розроблювання та експлуатації програмно-технічного забезпечення, крім цього вони знайомі з особливостями завдань, структурою та головним функціоналом та принципами програмно-технічного забезпечення ІБ, мають здатність використовувати мережеве обладнання та устаткування персоналу. До них належать:

- [I.B.1] ключовий персонал організації (користувачі та розробники);
- [I.B.2] персонал служб захисту інформації;
- [I.B.3] допоміжний персонал організації;
- [I.B.4] інженерно-технічний персонал організації (життєзабезпечення, експлуатація).

2.3.2. Техногенні джерела загроз ІБ

Техногенна група включає в себе джерела загроз, які визначаються техногенною діяльністю людства. Наслідки такої діяльності не контролюються людиною. Ці джерела небезпек є досить непередбачуваними, і тому потребують особливої уваги. Техногенні джерела загроз є досить актуальним на сьогоднішній день, оскільки в нинішніх умовах експерти прогнозують різке збільшення кількості технічних катастроф, які часто можуть бути спричинені фізичним та/або моральним старінням

обладнання, яке використовується, а також нестачею або відсутністю ресурсів на його оновлення або заміну.

Технічні засоби, які виступають потенційним джерелом загроз інформаційній безпеці, бувають зовнішні [II.A.]:

- [II.A.1] засоби зв'язку;
- [II.A.2] комунальні мережі (водопостачання, каналізація);
- [II.A.3] транспорт.

і внутрішні [II.B.]:

- [II.B.1] неякісне технічне забезпечення обробки інформації;
- [II.B.2] неякісне програмне забезпечення для обробки інформації;
- [II.B.3] допоміжні технічні засоби (охорона, сигналізація, телефонія);
- [II.B.4] інші технічні засоби, які використовують в установі;

2.3.3. Стихійні джерела загроз

Третя категорія джерел загроз ІБ поєднує обставини, що становлять форс-мажор, тобто такі об’єктивні та абсолютні обставини які поширюються та стосуються всіх. Форс-мажор у законодавстві та на практиці включає стихійні лиха чи інші непередбачувані обставини або події, яким практично неможливо запобігти на сучасному рівні людських знань та можливостей. Такі джерела небезпек є повністю непередбачуваними, і тому завжди слід застосовувати заходи захисту.

Природні або стихійні джерела ймовірних загроз ІБ розуміються в першу чергу як стихійні лиха [III.A.]:

- [III.A.1] пожежа;
- [III.A.2] землетрус;
- [III.A.3] повінь;
- [III.A.4] ураган;
- [III.A.5] різні непередбачувані обставини;
- [III.A.6] явища, які не можливо пояснити;
- [III.A.7] інші форс-мажорні обставини.

2.4. Класифікація вразливостей безпеки

Вразливості які є властивими об'єкту інформатизації, невіддільні від нього і через недоліки операційного процесу, властивостей архітектури систем, обмінних протоколів та інтерфейсів, програмно-апаратної платформи, умов роботи та розташування.

Джерела загроз доволі часто можуть використовувати вразливі місця для порушення ІБ та отримання неправомірної вигоди (заподіяння шкоди власнику або користувачу інформації).

Для кожної загрози можна зіставити різні вразливості. Усунення або значне ослаблення вразливостей впливає на здатність реалізовувати загрози інформаційної безпеки. Поділимо вразливі місця поділяються на класи (позначаються великими літерами), групи (римськими цифрами) та підгрупи (малими літерами). Вразливі місця інформаційної безпеки можуть бути:

- [A] об'єктивні;
- [B] суб'єктивні;
- [C] випадкові.

2.4.1. Об’єктивні вразливості

Об'єктивні вразливості як правило залежать від особливостей конструкції та технічних характеристик обладнання, що використовується на об'єкті, що охороняється. Повністю усунути ці вразливості неможливо, але їх можна значно послабити технічними та інженерними методами відбору загроз інформаційній безпеці. До них належать:

[A.I] ті, що стосуються технічних засобів які випромінюють:

- [A.I.a] електромагнітні технічні засоби (побічне випромінювання елементів технічних засобів, кабельних ліній, випромінювання на частотах генераторів та підсилювачів);

– [A.I.b] електричні технічні засоби (наведення електромагнітного випромінювання на лініях і провідниках, інфільтрація сигналів в ланцюзі живлення, в ланцюзі заземлення, нерівномірне споживання струму джерела живлення);
– [A.I.c] звукові технічні засоби (акустичний, віброакустичний).

[A.II] ті, що активуються:

– [A.II.a] апаратні закладки (встановлюються в телефонних лініях, в електромережі, в приміщеннях, в технічних засобах);
– [A.II.b] закладки програм (шкідливе програмне забезпечення, технологічні виходи з програм, нелегальні копії програмного забезпечення).

[A.III] ті, що визначаються характеристиками елементів:

– [A.III.a] елементи з електроакустичними перетвореннями (гучномовці та мікрофони, індуктори, дроселі, трансформатори тощо);
– [A.III.b] елементи, що піддаються дії електромагнітних полів (магнітні середовища, мікросхеми, нелінійні елементи, схильні до накладення ВЧ).

[A.IV] ті, що визначаються характеристиками об’єкта, що охороняється:

– [A.IV.a] розташування об’єкта (відсутність контрольованої зони, наявність прямої видимості об’єктів, віддалених та рухливих елементів об’єкта, вібраційні відображають поверхні)
– [A.IV.b] організація каналів обміну інформацією (використання радіоканалів, глобальних інформаційних мереж, орендованих каналів)

2.4.2. Суб’єктивні вразливості

[B.I] помилки:

– [B.I.a] у підготуванні та практичному використанні програмного забезпечення (при розроблюванні алгоритмів та ПЗ, установці та скачуванні ПЗ, при експлуатації ПЗ та введенні даних);
– [B.I.b] під час керування складними системами (під час використання можливостей систем самонавчання, налаштовування служб універсальних систем, організації керування потоком обміну інформацією);

– [B.I.c] при експлуатації технічних засобів (під час увімкнення / вимкнення технічних засобів, використання технічних засобів захисту, використання засобів обміну інформацією).

[B.II] порушення режимів:

– [B.II.a] охорони та захисту (доступ до об'єкта керування та певних технічних засобів);
– [B.II.b] роботи технічних засобів (енергопостачання, життєзабезпечення);
– [B.II.c] користування інформацією (обробка та обмін інформацією, зберігання та утилізації носіїв інформації);

2.4.3. Випадкові вразливості

Непередбачувані вразливості зазвичай залежать від довколишнього середовища та непередбачуваних умов. Ці фактори, як правило, непередбачувані і їх усунення є можливим лише при здійсненні сукупності організаційних та інженерних заходів для перешкоджання загрозам інформаційній безпеці системи:

[C.I] збої та відмови:

– [C.I.a] збої та несправності технічних засобів (наприклад, засоби обробки інформації, забезпечуючих ефективності засобів обробки інформації, забезпечуючих захист та контроль доступу);
– [C.I.b] застаріння та вихід з ладу носіїв інформації (знімні носії, жорсткі диски, елементи мікросхеми, кабелі та сполучні лінії);
– [C.I.c] збої програмного забезпечення (операційні системи та СУБД, програми, утиліти, антивірусні програми);
– [C.I.d] відключення електроенергії (обладнання для обробки інформації, допоміжне обладнання).

[C.II] ушкодження:

– [C.II.a] комунікації життєзабезпечення (електрика, вода, газ, тепло, каналізація, кондиціонування та вентиляція);

– [C.II.b] огороджувальні конструкції (зовнішні огорожі територій, стіни та стелі будівель, будівлі технологічного обладнання).

2.5. Класифікація загроз інформаційній безпеці системи розумного будинку

Після визначення необхідних даних була побудована класифікація загроз інформаційній безпеці технології "розумний будинок". Фрагмент отриманої класифікації представлений в табл. 2.2.

Висновки по розділу 2

У другому розділі визначено етапи розробки засобів захисту інформаційної безпеки розумного будинку та визначено найбільш ймовірні загрози. Виділено підсистеми розумного будинку, які використовуються у проектованій системі, визначено етапи методу моніторингу стану системи розумного будинку.

Розглянуто основні бездротові протоколи зв’язку, які використовуються в системах розумного будинку та наведено їх вразливості, та проблеми, та фактори, які можуть призвести до проблем з інформаційною безпекою, таких як взламування системи чи втрата конфіденційної інформації.

Проаналізовано загрози інформаційній безпеці та вразливості безпеки у системі розумного будинку. Джерела загроз та вразливості класифіковано на групи, по кожній з виділених груп наведено описання та приклади. Після визначення необхідних даних побудовано класифікацію загроз інформаційній безпеці та представлено фрагмент отриманої класифікації у вигляді таблиці.

Таблиця 2.2. Фрагмент класифікації загроз

Загроза (тип атаки)	**Джерело загрози**	**Вразливість**	**Вразливості безпеки інформації**	**Можливі наслідки**	**Підсистема**
Хакерські атаки на центральний сервер	I.A.1-6; I.B.1-4.	Підключення мережі РБ до Інтернету. Відсутність або неефективність механізмів захисту периметру мережі	A.I.a-b, A.II.a-b, A.III.b, A.IV.b, B.I.a-c, B.II.a, B.II.c, B.II.d C.I.a, C.I.c.	Порушення роботи або вихід з ладу центрального сервера і всієї системи. Порушення конфіденційності, цілісності та доступності інформації	Керування та зв'язку
Перехват інформації, яка передається про дротовим та бездротовим каналам зв'язку	I.A.1-6; I.B.1-4; II.A.1; II.B.1; II.B.2.	Можливість доступу зловмисника до дротових каналів або до зони перехвату радіосигналів мережі. Відсутність або неефективність механізмів захисту трафіку	A.I.a-b, A.II.a-b, A.III.a-b, A.IV.a-b, B.I.a-c, B.II.a-d, C.I.a-d, C.II.b.	Порушення конфіденційності інформації, яка передається по каналу. Можливий доступ до керування системою	Керування та зв'язку; безпеки та моніторингу; електроживлення; освітлення; опалення; вентиляції і кондиціювання; мультимедіа
Доступ зловмисника з правами адміністратора на центральний сервер	I.A.1-6; I.B.1-4.	Відсутність або неефективність механізмів аутентифікації та ідентифікації	A.I.a-b, A.II.a-b, A.III.a-b, A.IV.b B.I.a-c, B.II.a-d, C.I.a-d, C.II.a-b.	Порушення конфіденційності, цілісності та доступності інформації, яка знаходиться всередині мережі	Керування та зв'язку

РОЗДІЛ 3. РОЗРОБКА АЛГОРИТМІЧНОГО ТА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Проектування інформаційної системи полягає у визначенні функціональних вимог користувача системи, визначенні основних компонентів майбутньої системи та етапів її роботи, розробці алгоритмів. Для розробки описаних моделей використовується уніфікована мова моделювання UML.

3.1. Функціональні вимоги

Для опису функціональних вимог до розроблюваної системи була побудована діаграма прецедентів (рис. 3.1).

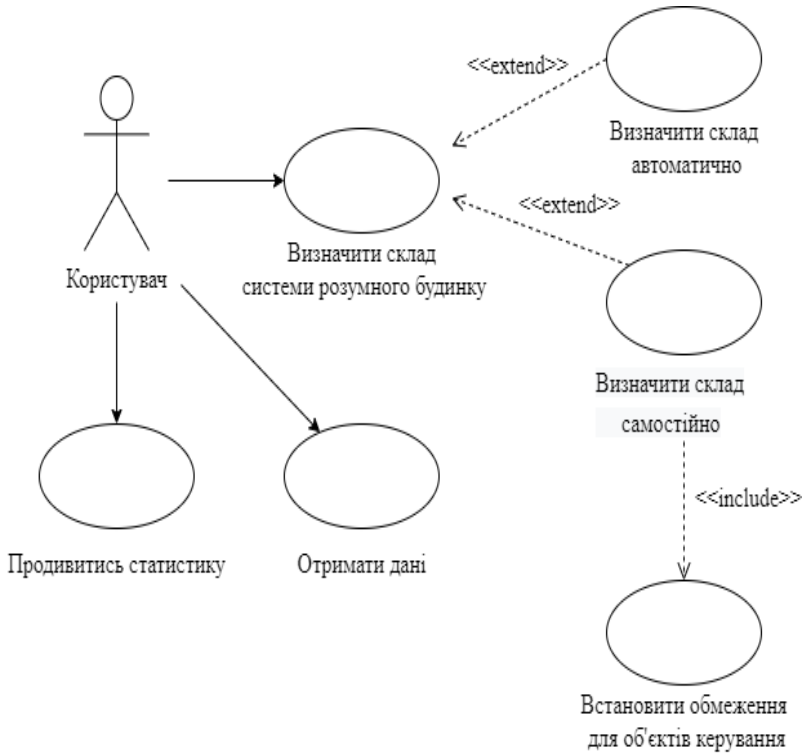


Рис. 3.1. Діаграма прецедентів для розроблюваної системи

Діаграма прецедентів показує основні функціональні вимоги:

1. Визначити систему розумного будинку:

а. автоматично;

b. визначити самостійно, встановлюючи при цьому обмеження для об'єктів керування;

2. Отримати дані про склад розумного будинку;

3. Переглянути статистику про виявлені загрози;

3.2. Компоненти системи

На основі функціональних вимог були виділені основні етапи роботи проектованої системи:

1. Визначення складу системи РБ і установка обмежень одним із способів:

a. автоматично;

b. додавання користувачем вручну кожного елемента системи РБ і обмежень для них.

2. Отримання даних з системи РБ.

3. Перевірка всіх отриманих даних (моніторинг) в режимі реального часу.

4. Генерація сповіщень про стан системи РБ.

На основі отриманих даних було визначено основні компоненти системи ІБ і побудована діаграма компонентів (рис. 3.2.).

Детальніше про обрані компонентах системи:

- компонент визначення системи необхідний для визначення складу системи РБ з отриманих даних;
- компонент представлення даних служить для відображення користувачу отриманих системою ІБ даних;
- компонент встановлення обмежень необхідний для автоматичного визначення обмежень для показів елементів системи РБ з отриманих даних;
- база даних служить для зберігання даних про склад системи РБ, класифікації загроз ІБ і даних, що використовуються системою ІБ;

– компонент моніторингу здійснює моніторинг стану системи РБ, шляхом перевірки вхідних даних і визначення невідповідностей;
– компонент сповіщень служить для інформування користувача про виявлені загрози або підозрілі дії;

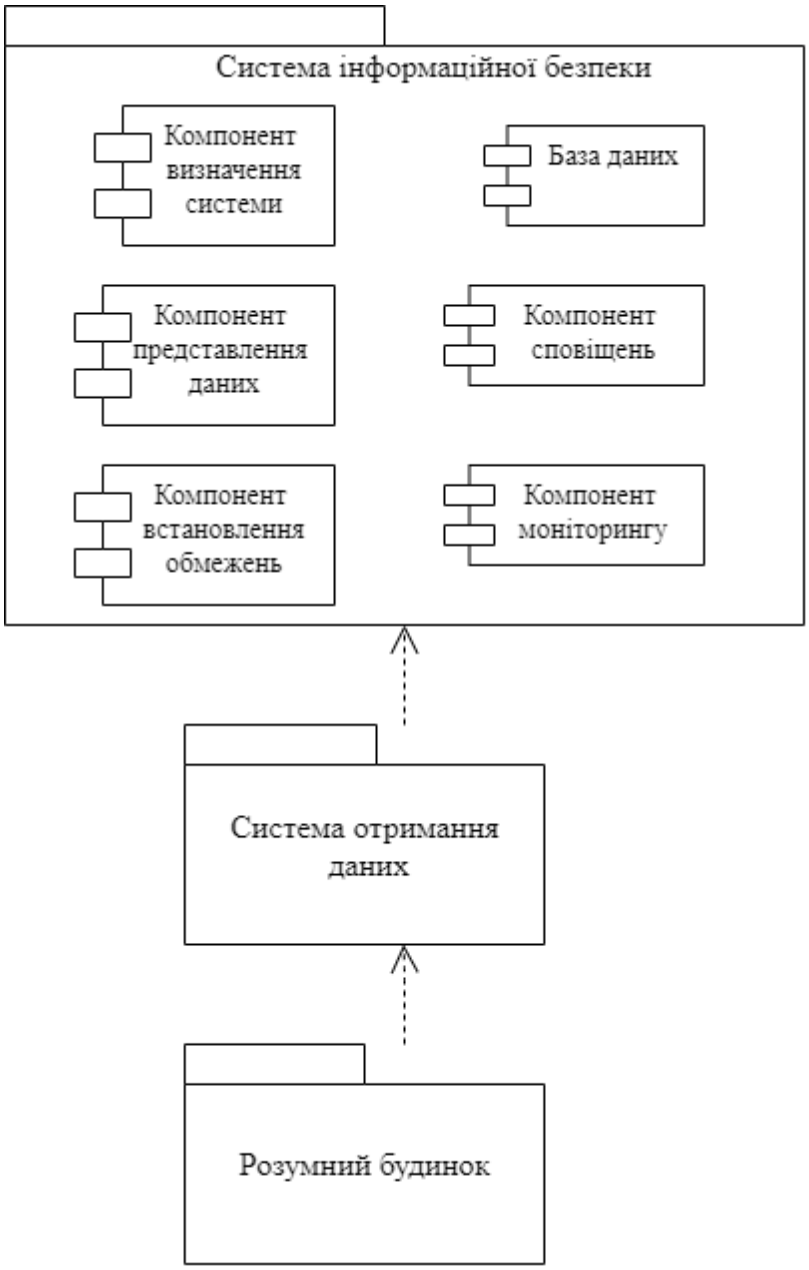


Рис. 3.2. Діаграма компонентів системи

3.3. Алгоритми системи

Після визначення функціональних вимог до системи інформаційної безпеки, основних етапів роботи системи і основних компонентів системи були розроблені алгоритми і побудовані діаграми діяльності для наступних основних дій системи ІБ:

1. Алгоритм визначення користувачем складу системи РБ і установки обмежень для об'єктів керування;
2. Алгоритм автоматичного визначення складу системи РБ і обмежень об'єктів керування;
3. Алгоритм моніторингу стану системи РБ.

3.3.1. Алгоритм визначення складу системи розумного будинку користувачем

Даний алгоритм виконується системою інформаційної безпеки при визначенні складу системи розумного будинку і встановленні обмежень шляхом додавання користувачем вручну кожного елемента системи РБ і обмежень для них. Для відображення алгоритму була побудована блок-схема, яка наведена у додатку А.

3.3.2. Алгоритм автоматичного визначення складу системи розумного будинку

Алгоритм виконується системою інформаційної безпеки при визначенні складу системи розумного будинку і встановленні обмежень. Для відображення алгоритму була побудована блок-схема, яка наведена у додатку Б.

3.3.3. Алгоритм моніторингу стану системи розумного будинку

Алгоритм полягає в перевірці всіх отриманих даних з системи розумного будинку в режимі реального часу. Для відображення алгоритму була побудована блок-схема, яка наведена у додатку В.

3.4. Структура опису даних в системі

У проектованій системі інформаційної безпеки для опису даних про склад системи розумного будинку, обмеженнях показань елементів системи і для опису загроз інформаційній безпеці обрано формат XML. Структури XML-файлів описано на мові XML-Schema.

3.4.1. Структура даних для опису складу системи розумного будинку

При визначенні складу системи розумного будинку користувачем самостійно, при визначення кожного елемента системи, формується XML-файл опису системи РБ. Графічне представлення схеми опису складу системи представлено у додатку Г.

Використовувані позначення:

- System - система розумного будинку;
- Subsystem - підсистема;
- Component - компонент підсистеми;
- Object - об'єкт керування;
- Sensor - датчик, Actuator - виконавчий механізм;
- Name - назва, Type - тип елемента;
- Min - мінімальне значення, Max - максимальне значення;
- Constraint - обмеження.

Наступні елементи мають атрибути:

- System, атрибут Name (назва системи розумного будинку);
- Subsystem, Component, Object, Sensor та Actuator мають атрибут ID (ідентифікатор);
- Constraint, атрибут Same (визначає чи є обмеження постійним);

3.4.2. Структура даних для автоматичного опису складу системи розумного будинку

При автоматичному способі визначення складу системи спочатку формується файл визначеної системи, потім розраховуються обмеження для елементів системи, і формується файл з описом складу системи. Графічне представлення файлу, що описує структуру файлу після автоматичного визначення складу системи представлено у додатку Ґ.

Використовувані позначення:

- System - система РБ;
- Subsystem - підсистема;
- Component - компонент підсистеми;
- Object - об'єкт керування;
- Sensor - датчик, Actuator - виконавчий механізм;
- Name - назва, Type - тип елемента;
- Min - мінімальне значення, Max - максимальне значення;
- Constraint - обмеження,
- Values/Value - значення / значення показів елемента.

Наступні елементи мають атрибути:

- System, атрибути: Name (назва системи РБ), DateFrom/DateTo (дата початку/дата закінчення збору даних), EverySec (інтервал збору даних), Round (ступінь округлення значення показів елемента);

- Subsystem/Component/Object/Sensor та Actuator мають атрибут ID - ідентифікатор;

- Constraint, атрибут Same - визначає чи є обмеження постійним;

- Value, атрибут DateTime - дата і час отримання даних;

3.4.3 Структура даних для опису загроз системі розумного будинку

Графічне представлення схеми опису загроз інформаційній безпеці системи розумного будинку представлено у додатку Д.

Використовувані позначення:

- Threats - загрози, Threat - загроза;
- Object - об'єкт керування;
- Sensor - датчик;
- Actuator - виконавчий механізм;
- Condition - умова;
- Consequences - можливі наслідки, Consequence - можливий наслідок;
- Sources - джерела, Source - джерело;
- Causes - можливі причини, Cause - можлива причина.

Наступні елементи мають атрибути:

- Object, атрибути SubsystemID (ідентифікатор підсистеми) і Name (назва);
- Condition, атрибути Type (тип відхилення) і ID (ідентифікатор);
- Threat, атрибути Name (назва загрози), ID;
- Consequence/Source/Cause мають атрибут ID.

Приклади типів відхилення від обмежень:

- Тип = 00 – будь-яке відхилення від обмежень;
- Тип = 1 відхилення: 0% – 20%;
- Тип = 2 відхилення: 20% – 40%;
- Тип = 3 відхилення: 40% – 60%;
- Тип = 4 відхилення: 60% – 80%;
- Тип = 5 відхилення: 80% – 100%;
- Тип = 100 відхилення: 100%.

3.5. Розробка програмного забезпечення системи

У розроблюваному додатку системи інформаційної безпеки для розумного будинку до описаних в попередньому розділі компонентів системи доданий компонент генерування даних. Даний компонент використовує файл-зразок, для визначення складу системи розумного будинку і значення показників об'єктів керування. Значення показників файлу зразка використовуються при генерації випадкових значень в генерованих файлах. Файли генеруються в окремому потоці програми. Рис. 3.3 демонструє потік генерування файлів (кожні дві секунди) з даними і запуску їх моніторингу.

```
//потік для генерування файлів даних та їх моніторингу
private static void ThreadStartGenerateFiles()
{
    while (do_generate)
    {
        mw.GenerateFile();//метод генерування файлів даних

        if (do_monitoring)
        {
            while (generated_files.Count != 0)//поки є файли для генерування
            {
                Monitoring();
            }
        }
        Thread.Sleep(2000); //2sec

    }
}
```

Рис. 3.3. Потік генерування і моніторингу файлів

Приклад згенерованого файлу зразка показаний на рис. 3.4.

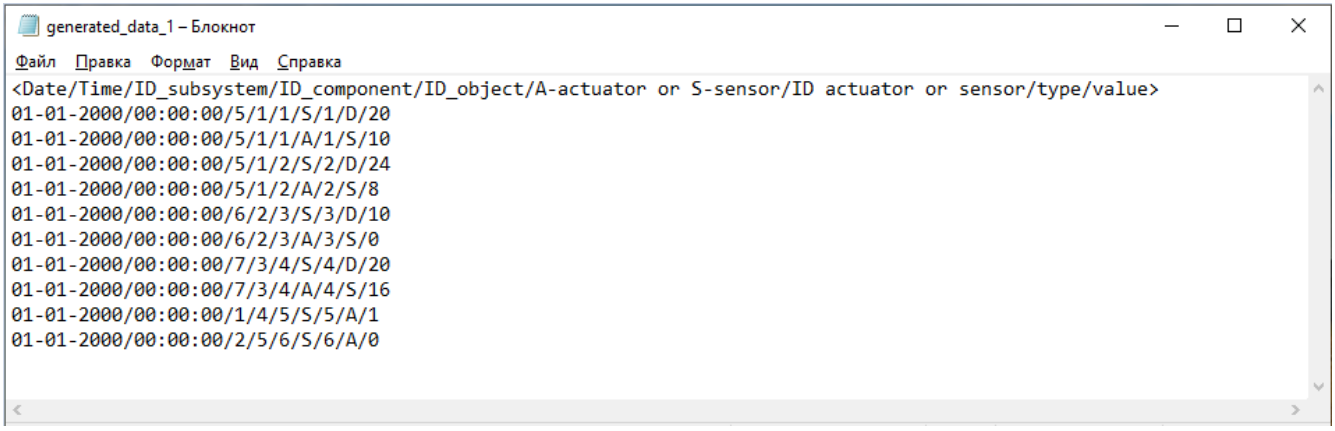


Рис. 3.4. Приклад файлу зразку

При запуску додатку необхідно визначити склад системи розумного будинку, після чого стануть доступні кнопки для запуску та зупинки моніторингу. Інтерфейс основного вікна до визначення складу системи представлений на рис. 3.5.

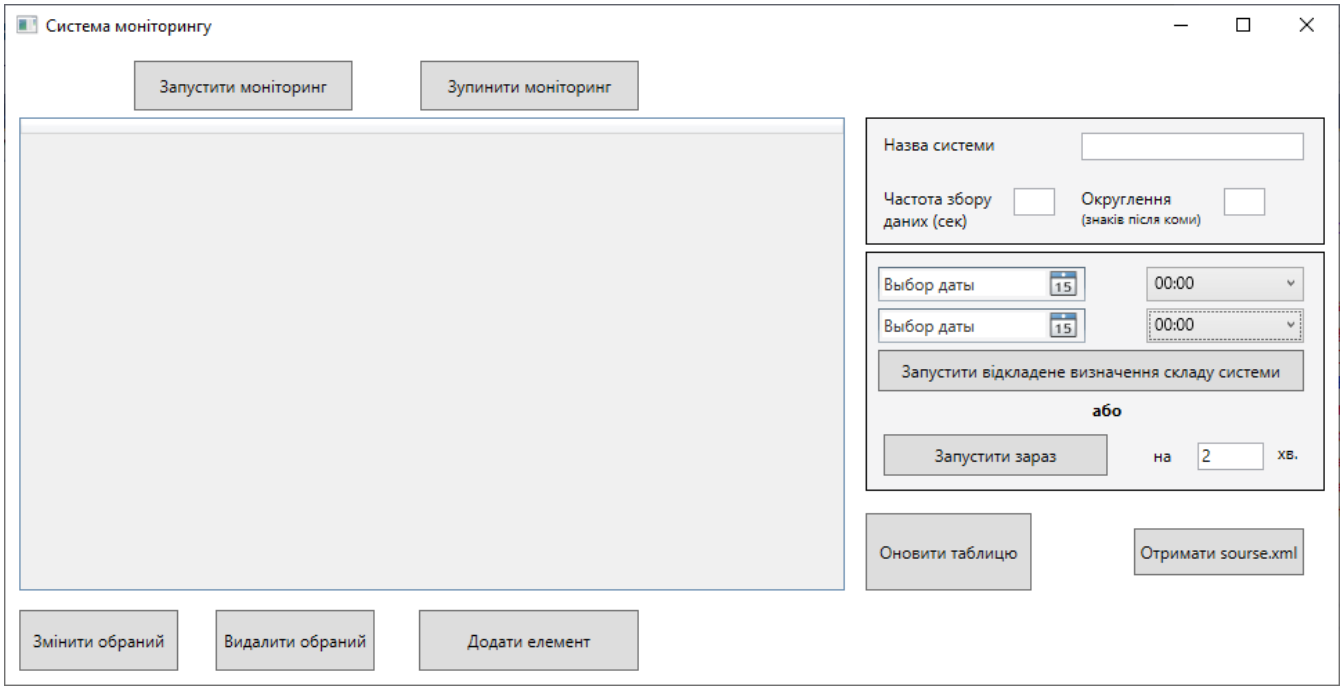


Рис. 3.5. Інтерфейс основного вікна до визначення складу системи

3.5.1. Автоматичне визначення складу системи розумного будинку

Для автоматичного отримання складу системи розумного будинку, необхідно в правій частині основного вікна визначити налаштування автоматичного визначення складу системи:

- вказати назву системи розумного будинку,
- визначити частоту збору даних (частота генерування файлів з даними),
- позначити дату і час початку та закінчення відкладеного збору даних або визначити час закінчення для збору даних в поточний момент часу.

Панель налаштування автоматичного збору даних показана на рис. 3.6.

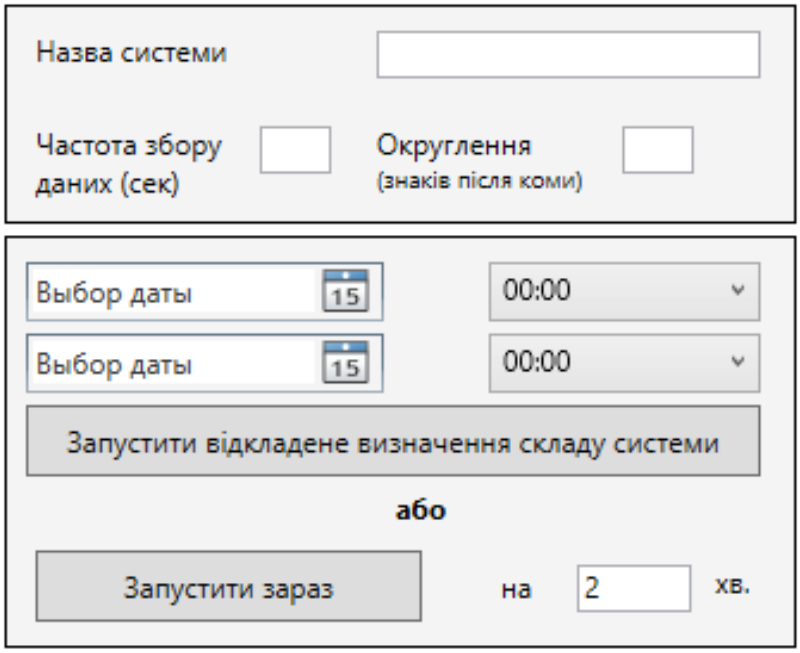


Рис. 3.6. Панель налаштування автоматичного збору даних

На рис. 3.7. показано фрагмент коду, який додає елементи датчик або виконавчий механізм і дані елементів в XML-файл структури отриманої системи.

```
//додавання нового елемента з одним значенням
if (xdoc.Descendants(elem_tagname).Where(x => x.Attribute("ID").Value == elem_id).Count() == 0)
{
    XmlElement elem = doc.CreateElement(elem_tagname);
    elem.SetAttribute("ID", elem_id);
    root_for_element.AppendChild(elem);
    XmlElement elem1 = doc.CreateElement("Type");
    string type_ = "";

    if (elem_tagname == "Actuator")//виконавчий механізм
    {
        type_ = Actuator_types[type];
    }
    else if (elem_tagname == "Sensor")//датчик
    {
        type_ = Sensor_types[type];
    }
    elem1.InnerText = type_;
    elem.AppendChild(elem1);
    XmlElement elem2 = doc.CreateElement("Values");
    elem.AppendChild(elem2);
    element_for_value = elem2;
    XmlElement elem3 = doc.CreateElement("Value");
    elem3.SetAttribute("DateTime", date + "T" + time);
    elem3.InnerText = value; elem2.AppendChild(elem3);
    }
    else //Додавання наступних отриманих значень елемента
        {
            xpath = "System/Subsystem[@ID='" + subsystem_id + "']/Component[@ID='" +
            component_id + "']/Object[@ID='" + object_id + "']/" +
            elem_tagname + "[@ID='" + elem_id + "']/Values";
            XmlElement elem4 = doc.CreateElement("Value");
            elem4.SetAttribute("DateTime", date + "T" + time);
            elem4.InnerText = value;
            doc.SelectSingleNode(xpath).AppendChild(elem4);
        }
```

Рис. 3.7. Фрагмент методу додавання елементів

3.5.2 Визначення складу системи розумного будинку

Для самостійного визначення користувачем складу системи розумного будинку необхідно на основному вікні вибрати кнопку "додати елемент", після чого відкриється вікно для додавання/редагування елемента. Інтерфейс вікна додавання/редагування елемента представлений на рис. 3.8.

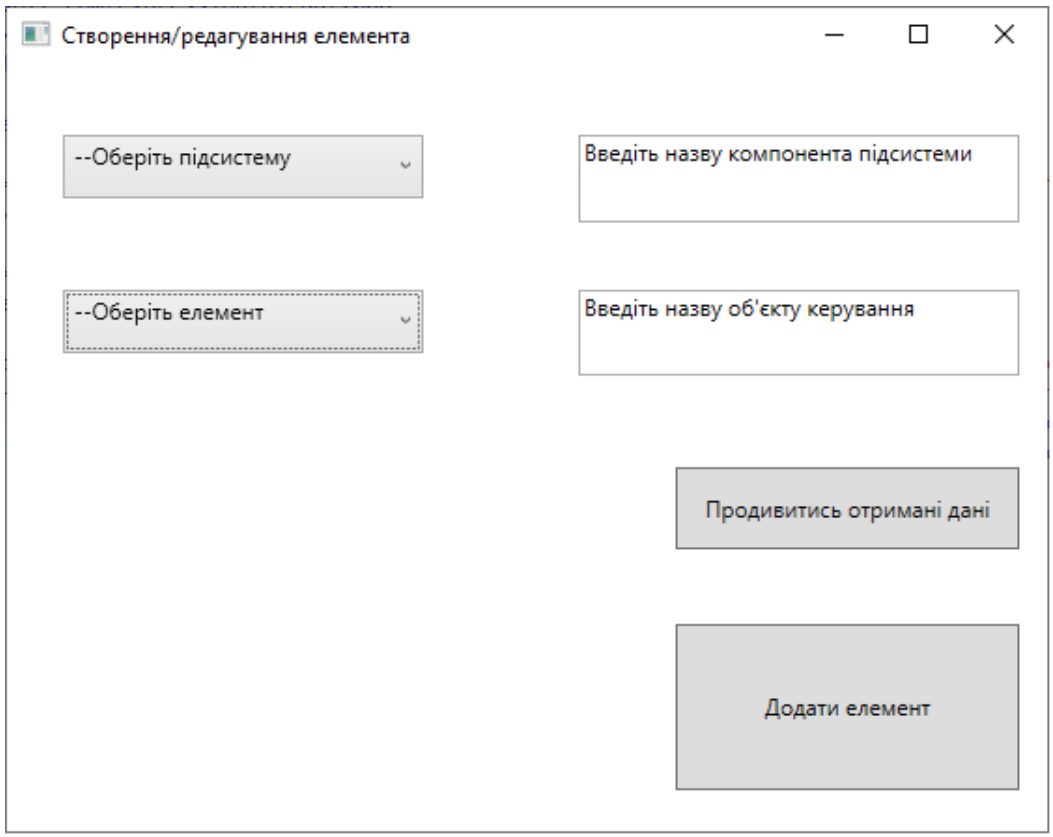


Рис. 3.8. Інтерфейс вікна додавання елемента

Користувачу необхідно обрати зі списку підсистему, ввести назву для компонента підсистеми і об'єкта керування (або вибрати з існуючих, якщо вони були додані раніше), вибрати створюваний елемент. Після вибору елемента, стане доступним випадаючий список для визначення типу елемента, текстові поля для визначення обмежень, та допустимого відхилення від обмежень. Приклад заповненої форми для створення датчика елемента керування батареї представлений на рис. 3.9.

Після визначення складу системи в таблиці на головному вікні додатку з'являться дані про елементи. Дані в таблиці можна сортувати по спаданню і по зростанню будь-якого стовпчика. Приклад заповненої таблиці з даними представлений на рис. 3.10.

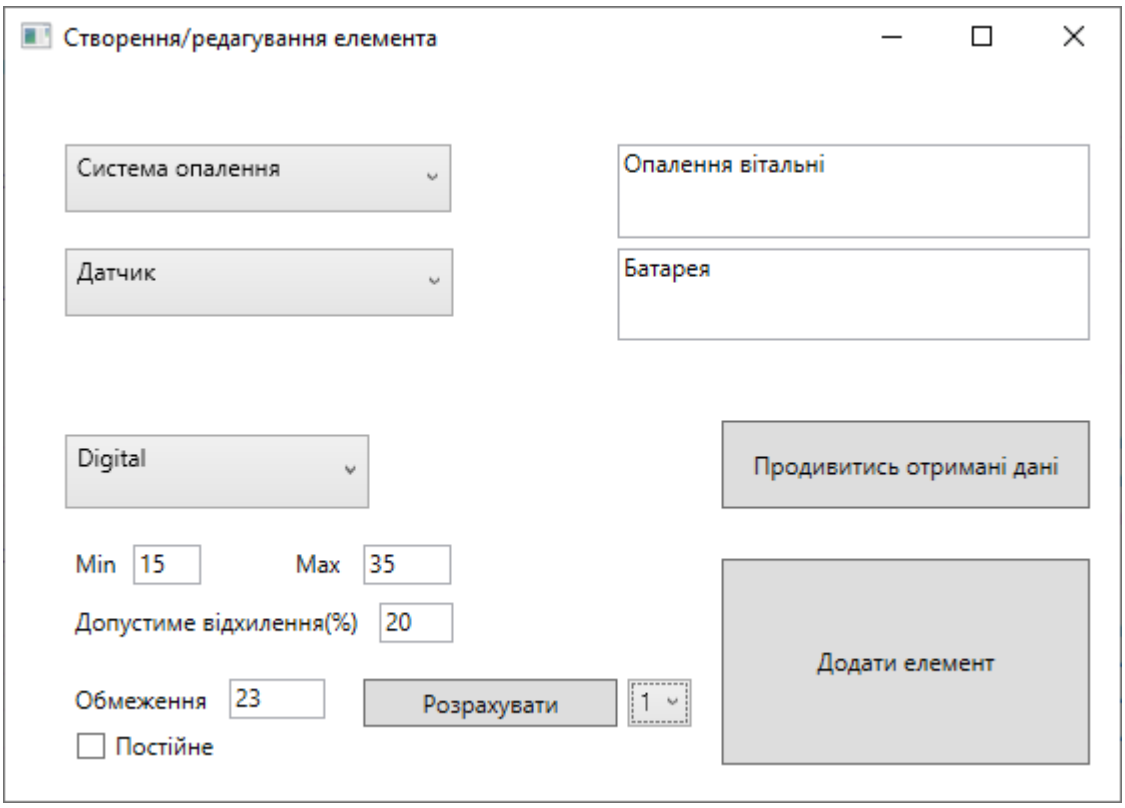


Рис. 3.9. Інтерфейс заповненого вікна додавання елемента

SubsystemName	SubsystemID	ComponentName	ComponentID	ObjectName	ObjectID	Constraint	Min	Max	ID	Type	Name	State
Система опалення	5	Опалення вітальні	1	Батарея	1	23	15	35	1	Digital	Sensor	green
Система опалення	5	Опалення вітальні	1	Батарея	1	20	--	--	1	Switch	Actuator	green
Система опалення	5	Опалення спальні	1	Батарея	2	20	14	32	2	Digital	Sensor	green
Система опалення	5	Опалення спальні	1	Батарея	2	18	--	--	2	Switch	Actuator	green
Система вентиляції	6	Вентиляція вікон	2	Вікно	3	15	0	30	3	Digital	Sensor	green
Система вентиляції	6	Вентиляція вікон	2	Вікно	3	15	--	--	3	Switch	Actuator	green
Система кондиціонування	7	Кондиціонування вітальні	3	Кондиціонер	4	18,5	16	30	4	Digital	Sensor	green
Система кондиціонування	7	Кондиціонування вітальні	3	Кондиціонер	4	16	--	--	4	Switch	Actuator	green
Система керування та зв'язку	1	Сервер	4	Системний блок	5	1	0	1	5	Analog	Sensor	green
Система безпеки та моніторингу	2	Підсистема безпеки	5	Розумний замок	6	1	0	1	6	Analog	Sensor	green

Рис. 3.10. Таблиця з даними

На рис. 3.11 продемонстровано метод для заповнення таблиці даними з XML-файлу зі складом системи розумного будинку.

```
private void Fulltable() //заповнення таблиці даними з source.xml
{   // дані з xml
    XDocument doc = XDocument.Load(path);
    var result = doc.Descendants("Constraint").Select(x => new
    {
        SubsystemName = x.Parent.Parent.Parent.Parent.Element("Name").Value,
        SubsystemID = x.Parent.Parent.Parent.Parent.Attribute("ID").Value,
        ComponentName = x.Parent.Parent.Parent.Element("Name").Value,
        ComponentID = x.Parent.Parent.Parent.Attribute("ID").Value,
        ObjectName = x.Parent.Parent.Element("Name").Value,
        ObjectID = x.Parent.Parent.Attribute("ID").Value,
        Constraint = x.Value,
        Min = x.Parent.Element("Min") != null ? x.Parent.Element("Min").Value : "--",
        Max = x.Parent.Element("Max") != null ? x.Parent.Element("Max").Value : "--",
        ID = x.Parent.Attribute("ID").Value,
        Type = x.Parent.Element("Type").Value,
        Name = x.Parent.Name.ToString(),
        State = "green"
    });
    dgrid.ItemsSource = result; //заповнюємо таблицю

    elements_count = dgrid.Items.Count; //записуємо кількість елементів системи РБ
    //заповнюємо списки з наявними ID підсистем, компонентів, об'єктів, елементів
    FullLists();

}
```

Рис. 3.11. Метод для заповнення таблиці даними з XML-файлу

Такі дані елементів як назва, мінімальне та максимальне значення та обмеження можна змінювати, для цього необхідно виконати подвійне натискання на необхідному значенні в таблиці або вибрати рядок в таблиці і натиснути кнопку "Змінити обраний". У першому варіанті відкриється вікно для редагування конкретного значення даних елемента (рис. 3.12), у другому відкриється заповнене даними елемента вікно створення / редагування елемента, описане раніше.

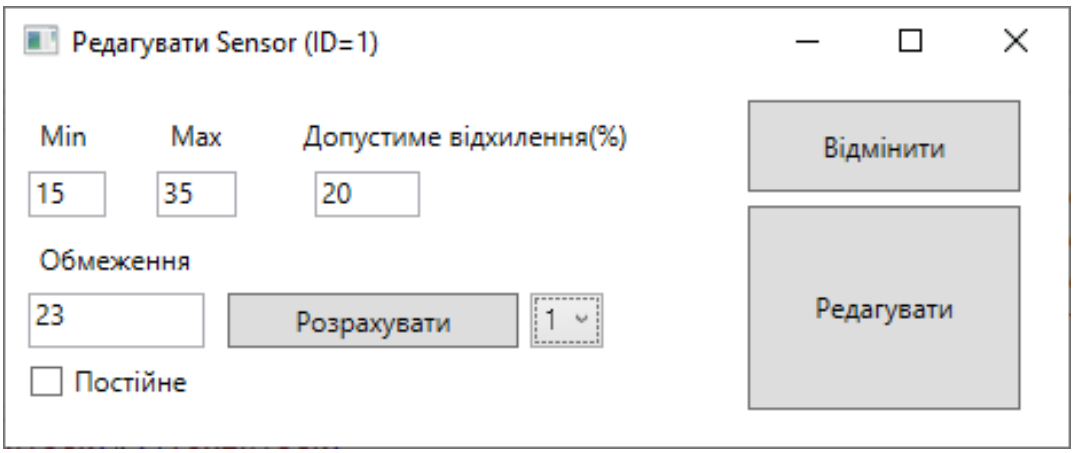


Рис. 3.12. Приклад редагування параметрів датчика

3.5.3. Моніторинг стану системи розумного будинку

Для запуску моніторингу стану системи РБ на головному вікні необхідно вибрати кнопку "Запустити моніторинг". При необхідності моніторинг стану РБ можна зупинити, вибравши кнопку "Зупинити моніторинг". При виявленні загроз і невідповідності показань датчика або виконавчого механізму об'єктів керування, в таблиці з даними змінюється значення елемента в стовпці "State" (статус) і рядок елемента підсвічується кольором. Приклад вигляду таблиці з даними, в яких виявлені загрози, показаний на рис. 3.13.

SubsystemName	SubsystemID	ComponentName	ComponentID	ObjectName	ObjectID	Constraint	Min	Max	ID	Type	Name	State
Система опалення	5	Опалення вітальні	1	Батарея	1	23	15	35	1	Digital	Sensor	red
Система опалення	5	Опалення вітальні	1	Батарея	1	20	--	--	1	Switch	Actuator	green
Система опалення	5	Опалення спальні	1	Батарея	2	20	14	32	2	Digital	Sensor	green
Система опалення	5	Опалення спальні	1	Батарея	2	18	--	--	2	Switch	Actuator	green
Система вентиляції	6	Вентиляція вікон	2	Вікно	3	15	0	30	3	Digital	Sensor	red
Система вентиляції	6	Вентиляція вікон	2	Вікно	3	15	--	--	3	Switch	Actuator	green
Система кондиціонування	7	Кондиціонування вітальні	3	Кондиціонер	4	18,5	16	30	4	Digital	Sensor	red
Система кондиціонування	7	Кондиціонування вітальні	3	Кондиціонер	4	16	--	--	4	Switch	Actuator	green
Система керування та зв'язку	1	Сервер	4	Системний блок	5	1	0	1	5	Analog	Sensor	red
Система безпеки та моніторингу	2	Підсистема безпеки	5	Розумний замок	6	1	0	1	6	Analog	Sensor	green

Рис. 3.13. Приклад вигляду таблиці зі знайденими загрозами

Метод для визначення загрози показано на рис. 3.14.

```
private static int GetThreatID(string tagname, string elemid, int dev)//визначення ID загрози
    {
        int threat_id = -1;
        XDocument xdoc = XDocument.Load(path);
        string name="";

        switch (tagname)
        {
            case ("S"):
                tagname = "Sensor";
                break;
            case ("A"):
                tagname = "Actuator";
                break;
        } //отримуємо назву об'єкту, в якому знайдено загрозу

        var v = xdoc.Descendants("Object").Where(x =>
        x.Element(tagname).Attribute("ID").Value == elemid).Elements("Name");
        foreach (XElement e in v)
        { name = e.Value; }
        XmlDocument doc = new XmlDocument();
        doc.Load("..\\..\\threat.xml");
        if (doc.SelectSingleNode("//Object[@Name='" + name +
    "']//'" + tagname + "'//Condition[@Type='" + GetConditionType(dev) + "']") != null)
        //якщо у threat.xml є об'єкт з заданою умовою
        {
            threat_id = Convert.ToInt32(doc.SelectSingleNode("//'" + tagname +
    "'//Condition[@Type='" + GetConditionType(dev) + "']//Threat/@ID").Value);
        }
        if (doc.SelectSingleNode("//Object[@Name='" + name + "']//'" + tagname +
            "'//Condition[@Type='" + "00" + "']") != null)
        {
            threat_id = Convert.ToInt32(doc.SelectSingleNode("//'" + tagname +
    "'//Condition[@Type='" + "00" + "']//Threat/@ID").Value);
        }
        return threat_id;
    }
```

Рис. 3.14. Метод визначення загрози

Список типів можливих помилок:

– Помилка в форматі дати;
– Помилка в форматі часу;
– Помилка в форматі ID підсистеми / компонента / об'єкта;
– Помилка в форматі ID елемента;
– Помилка в форматі типу елемента
– Помилка в форматі значення елемента;

– Не вдалося знайти компонент / підсистему з заданим ID;
– Не вдалося знайти об'єкт / датчик / виконавчий механізм із заданим ID;
– У датчика з заданим ID невідомий тип;
– Невірний тип датчика/виконавчого механізму;
– У виконавчого механізму з заданим ID невідомий тип;
– Дані сенсора не відповідають обмеженням;
– Неправильна кількість елементів даних;
– У вхідному масиві відсутні дані по підсистемі / компоненту / об’єкту / датчику / виконавчому механізму.

Подвійне натискання на статус елемента відкриває вікно з детальними відомостями про можливу загрозу. Приклад відомостей про загрозу, виявлену у системному блоці сервера системи управління, представлений на рис. 3.15.

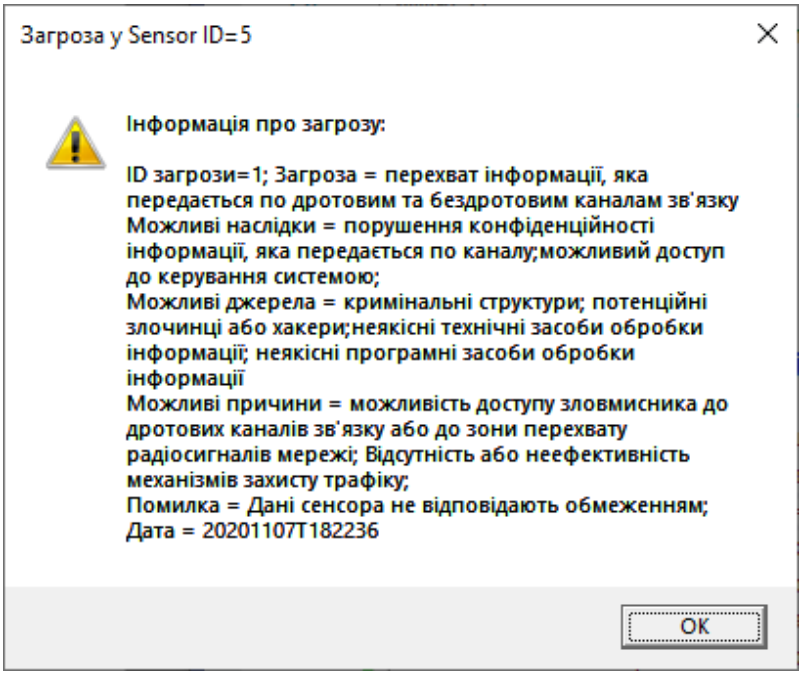


Рис. 3.15. Вікно з відомостями про можливі загрози

При відсутності даних про загрозу система інформаційної безпеки надає користувачу дані про помилку та дату її знаходження. Приклад відомостей про невідому загрозу, виявлену у датчику відкриття вікна, представлений на рис. 3.16.

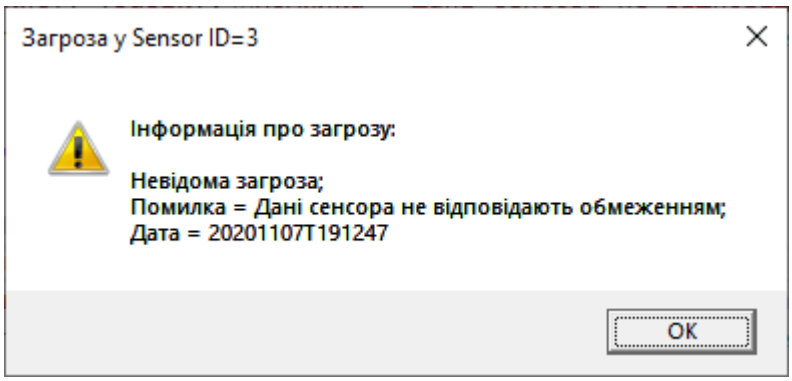


Рис. 3.16. Вікно з відомостями про невідому загрози

Висновки по розділу 3

У третьому розділі визначено функціональні вимоги до розроблюваної системи, на їх основі визначені та описані компоненти системи. Розроблено алгоритми роботи системи, такі як: алгоритм визначення складу системи самостійно користувачем та автоматично, алгоритм моніторингу стану системи розумного будинку.

Спроектовано структуру опису даних в системі та побудовано схеми роботи з даними: схема опису складу системи розумного будинку, схема опису автоматичного визначення складу системи та схема опису загроз.

Розроблено додаток який проводить моніторинг системи розумного будинку, виявляє загрози та виводить інформацію про загрозу: можливі джерела загрози, можливі причини та наслідки. Розроблений продукт дає змогу користувачу самостійно визначити склад системи, та обмеження, або визначає їх автоматично, даний додаток можна використовувати для будь-якої системи розумного будинку, що застосовуються в житлових приміщеннях.

РОЗДІЛ 4. МАРКЕТИНГОВИЙ АНАЛІЗ СТАРТАП-ПРОЄКТУ

4.1. Опис ідеї проєкту

Таблиця 4.1. Опис ідеї стартап-проєкту

Зміст ідеї	Напрямки застосування	Вигоди для користувача
Система моніторингу та оцінки загроз інформаційній безпеці розумного будинку	Використання додатку у системах розумного будинку для забезпечення інформаційної безпеки	Функціональна потужність та можливість налаштування системи від індивідуальні потреби, простота експлуатації, яка не потребує спеціальних знань та навичок, відносно невисока ціна продукту

Таблиця 4.2. Опис ідеї стартап-проєкту

№	Техніко-економічні характери-тики ідеї	Продукція конкурентів				W (слабка сторона)	N (нейтральна сторона)	S (сильна сторона)
		Мій проєкт	Dojo	CUJO	Bitdefender Box			
1	Якість дизайну	С	В	В	С		+	
2	Зручність використання	С	В	В	В	+		
3	Вимоги до системи	Н	С	С	С			+
4	Можливість настройки роботи	В	Н	Н	Н			+
5	Функціональна потужність	В	Н	Н	С			+

4.2. Технологічний аудит ідеї проєкту

Таблиця 4.3. Технологічна здійсненність ідеї проєкту

№	Ідея проєкту	Технології її реалізації	Наявність технологій	Доступність технологій
1	Розробка системи Система моніторингу та оцінки загроз інформаційній безпеці розумного будинку	Використання інструмента Windows Presentation Foundation (WPF)	Наявна. Має велику кількість готових програмних інструментів для вирішення різних проблем. Має гарно розроблені бібліотеки, конструктор.	Вільна
		Використання мови програмування C#	Наявна. Має основні простори імен для модуля	Вільна
		Використання мови програмування Python	Наявна. Має один фреймворк	Вільна
Обрана технологія реалізації ідеї проєкту: WPF, мова програмування: C#				

Система WPF обрана через можливості використання будь-якої .NET-сумісної мови програмування разом з мовою XAML. WPF і XAML об'єднуються в повнофункціональну систему подання для створення візуально привабливих класичних додатків Windows, що включають в себе користувальницький інтерфейс, мультимедіа та складні бізнес-моделі.

Мова програмування C # має кілька класів для ефективної і швидкої роботи з XML-документами, які обираються в залежності від поставлених завдань.

4.3. Аналіз ринкових можливостей запуску стартап-проєкту

Таблиця 4.4. Попередня характеристика потенційного ринку

№	Показники стану ринку	Характеристика
1	Кількість головних гравців, од	4
2	Загальний обсяг продаж, грн./ум.од	100 тис. долларів США на рік
3	Динаміка ринку	Ринок систем безпеки для розумного будинку зростає з кожним роком
4	Наявність обмежень для входу	Відсутні, відкритий ринок
5	Специфічні вимоги до стандартизації та сертифікації	Відсутні
6	Середня норма рентабельності в галузі або по ринку, %	70%

Висновок: враховуючи кількість головних гравців по ринку, зростаючу динаміку ринку, невелику кількість конкурентів та середню норму рентабельності можна зробити висновок, що на даний момент, ринок для входження стартап-продукту є привабливим.

Таблиця 4.5. Характеристика потенційних клієнтів стартап-проєкту

№	Потреба, що формує ринок	Цільова аудиторія	Відмінності у поведінці цільових груп клієнтів	Вимоги споживачів до товару
1	Потреба захисту інформаційної безпеки у розумному будинку	Фізичні особи	Як правило, користуються системами розумного будинку з низьким рівнем захисту інформації	Зручність у використанні, точність роботи, надійність, швидка робота системи. Спроможність швидко освоїтись як користуватись системою.
		Підприємства	Використовують тільки системи, вироблені спеціалізованими компаніями, з достатнім рівнем захисту;	

Таблиця 4.6. Фактори загроз

№	Фактор	Зміст загрози	Можлива реакція компанії
1	Конкуренти	Наявність конкурентів котрі надають схожі рішення	Зменшення ціни на поставлену послугу; Розробка унікальних характеристик товару; Надання ліцензій на обслуговування
2	Кошти на розробку та підтримку продукту	Закінчення грошей та недостатнє фінансування	Залучення додаткових інвесторів, мотивація роботи на перспективу; Ітеративна розробка продукту задля покрокового виведення продукту на ринок та отримання відповіді користувачів
3	Вихід аналогу	Вихід аналогу даного товару може призвести до знецінення та безідейності даного товару	Вихід товару на ринок в коротші строки з не повною, але достатньою, функціональністю для зацікавлення усіх цільових аудиторій; Проведення рекламної компанії

Таблиця 4.7. Фактори можливостей

№	Фактор	Зміст можливості	Можлива реакція компанії
1	Новий продукт	Вихід на ринок, Зменшення монополії, Надання нових рішень у сфері	Розробка нової функціональності; Вихід нової продукції на ринок; Надання різноманітних типів ліцензій в залежності від потреб користувача \ замовника.
2	Вихід аналогу	Надати продукт з певними характеристиками та можливостями що відсутні у компаній конкурентів	Аналіз ринку та користувачів задля задоволення їх потреб та надання функціональності у найкоротші строки за ціну, котра є дешевшою ніж у продуктів-замінників.
3	Зворотній зв’язок від користувачів	Можливість отримання необхідної інформації для вдосконалення продукту	Наявність вхідних даних та реакція на них з боку команди розробників задля задоволення потреб та бажань кінцевих користувачів системи моніторингу та оцінки загроз розумного будинку.
4	Грошова винагорода за рекламу	При достатньому попиту на систему моніторингу та оцінки загроз інформаційній безпеці розумного будинку можлива комерціалізація продукту на основі реклами задля отримання грошової винагороди для подальшого розвиту продукту та оплати заробітної плати працівникам	Точкова комерціалізація продукту; Введення реклами; Ведення додаткових коштів у проект задля його подальшого розвитку.

Таблиця 4.8. Ступеневий аналіз конкуренції на ринку

№	Особливості конкурентного середовища	В чому проявляється дана характеристика	Вплив на діяльність підприємства (можливі дії компанії, щоб бути конкурентоспроможною)
1	Тип конкуренції: монополістична	Товар від кожної компанії на ринку, являється недосконалим замінником товару, реалізованого іншими фірмами; На ринку є умови для входу та виходу; Ціна корелює між суперниками;	Розробка продукту з характеристиками, які покривають сфери вживання що не покривають інші товари-замінники; Кореляція цін у відповідності до товарів замінників; Різни типи ліцензій.
2	Рівень конкурентної боротьби: світовий	Всі продукти замінники розроблялись інтернаціональними командами з різних куточків світу, продукти не належать до певної держави, а належать команді розробників	Вихід на ринок збуту продукту з клієнто-необхідною функціональністю; Налагодження маркетингу на основних Інтернет ресурсах задля охоплення великої кількості потенційних користувачів; Надання бета-версій продукту.
3	Галузева ознака: внутрішньогалузева	Даний тип продукту може використовуватися тільки у сфері розробки ІТ додатків \ продуктів	Надання зручного, інтуїтивно зрозумілого інтерфейсу; Підтримка всім відомих методів взаємодії з середовищем розробки; Наявність документації та онлайн підтримки.
4	Конкуренція за видами товарів: товарно-видова	Дана конкуренція – конкуренція між товарами одного виду.	Впровадження функціональності яка відсутня у товарів-замінників; Спрощення інтерфейсів; Надання підтримки.
5	Характер конкурентних переваг: цінова та не цінова	Цінові переваги – точкова комерціалізація; Не цінова – надання функціональності, що відсутня у товарах-замінниках.	Надання платних ліцензій лише на критично важливу функціональність для клієнта з певним строком підтримки, що зазначена у відповідній ліцензії; Впровадження унікальної функціональності.
6	За інтенсивністю: марочна	Наявність унікального знаку що відрізняє даний продукт від продуктів-замінників	Впровадження власної назви та власного знаку.

Таблиця 4.10. Аналіз конкуренції в галузі за М. Портером

Складові аналізу	Прямі конкуренти в галузі	Потенційні конкуренти	Постачальники	Клієнти	Товари-замінники
	Середня	Низька	Низька	Середня	Середня
Висновки	На даний час конкурентів в даній області невелика кількість в порівнянні з розмірами ринку клієнтів для системи	Можлива поява нових подібних розробок для, але прогрес у цьому напрямку не дуже стрімкий	Немає залежності від постачальників, так як використовується програмне забезпечення, яке розроблене власноруч без додаткових постачань від третіх осіб	Клієнти можуть диктувати умови на ринку через повідомлення на форумах або в полі відгуків в точках продажу додатку	Середня ймовірність появи нових систем, можливість введення стандартизації систем інформаційної безпеки в розумному будинку

Проаналізувавши можливості роботи на ринку з огляду на конкурентну ситуацію можна зробити висновок: оскільки кожний з існуючих продуктів не впливає у великій мірі на поточну ситуацію на ринку в цілому, кожний з існуючих продуктів має свою специфічну сферу використання та свої позитивні та негативні сторони щодо рішення певних типів задач, то робота та вихід на даний ринок є можливою і реалізованою задачею.

Для виходу на ринок продукт повинен мати функціонал що відсутній у продуктів-аналогів, повинен задовольняти потреби користувачів, мати необхідний та достатній функціонал з конфігурування, підтримку зі сторони розробників та можливість розробки спеціального функціоналу за відповідною ліцензією.

Таблиця 4.11. Обґрунтування факторів конкурентоспроможності

№	Фактор конкурентоспроможності	Обґрунтування
1	Прагматичність	Через запуск стартапу система буде не дуже складно з точки зору архітектури перший час. Через певний період із додаванням функціоналу та оптимізації алгоритмів роботи програмний код буде все складнішим. Такий етап наступить не раніше одного року постійної роботи над проектом.
2	Зручність	Оскільки стартап розробляється на багатьох платформах з різною шириною екранів, то зручність використання системи на різних пристроях буде відігравати не малу роль у спроможності конкурувати з іншими гравцями ринку
3	Швидкість роботи	Швидкість роботи відіграє велику роль для користувачів, оскільки вони не будуть готові чекати декілька хвилин на виведення результату роботи додатку.
4	Оптимізація	Якщо додаток буде дуже часто видавати помилки при роботі, то користувачі не будуть вважати додаток надійним
5	Приватність	В останні роки приватність людей та інформація щодо них все частіше зловживається шахраями або великими корпораціями, які потребують погодження з умовами доступу до приватної інформації та її обробки.
6	Технічна підтримка	Якщо технічна підтримка компанії буде працювати своєчасно та швидко, то це допоможе зберегти репутацію компанії на відміну від конкурентів, де їй не приділяють увагу.

Таблиця 4.12. Порівняльний аналіз сильних та слабких сторін системи

	Фактор конкурентоспроможності	Бали 1-20	Рейтинг товарів-конкурентів у порівнянні з запропонованим						
			-3	-2	-1	0	+1	+2	+3
	Зручність використання	17				+			
	Якість дизайну	12					+		
	Можливість налаштування системи	18	+						
	Функціональна потужність	17		+		+			
	Простота експлуатації	13					+		
	Якість та зрозумілість інтерфейсу	13					+		

SWOT-аналіз дає чітке уявлення про фактори зовнішнього і внутрішнього середовища і вказує, в яких напрямках потрібно діяти, використовуючи сильні сторони, щоб максимізувати можливості і звести до мінімуму загрози і слабкі сторони. За допомогою цього методу можна позначити основні проблеми проєкту, визначити шляхи вирішення і перспективу розвитку.

Таблиця 4.13. SWOT аналіз стартап-проєкту

Сильні сторони (S):	Слабкі сторони (W):
– Функціональна потужність; – Можливість налаштування під індивідуальні вимоги споживача; – Відносно невисока ціна. – Відсутність додаткового збору даних.	– Невисока якість дизайну; – Недостатня простота експлуатації.
Можливості (O):	Загрози (T):
– Зростання кількості користувачів систем розумного будинку для житлових будинків. – Підвищення обізнаності користувачів систем розумного будинку про необхідність захисту інформаційної безпеки їх систем.	– Відсутність попиту на дану розробку. – Жорсткість вимог в законодавстві щодо програмних продуктів та інформаційних технологій. – Розвиток конкурентних розробок.

Таким чином, в результаті SWOT-аналізу були розглянуті сильні і слабкі сторони розробки, можливості та можливі загрози. Основні слабкі сторони наукової розробки це низька якість дизайну і складність експлуатації. У першому випадку при будь-яких можливостях та загрозах слід звернутися до дизайнера. У другому - постаратися спростити експлуатацію продукту. Крім зміни попиту одночасно джерелом можливостей і загроз є законодавство: введення обмеження для іноземного ПЗ може значно підвищити попит на розробку, знизивши конкуренцію, посилення вимог для розроблюваних ПЗ може вимагати переробки або доопрацювання частини функціоналу продукту.

Таблиця 4.14. Альтернативи ринкового впровадження стартап-проєкту

№	Альтернатива (орієнтовний комплекс заходів) ринкової поведінки	Ймовірність отримання ресурсів	Строки реалізації
1	Безкоштовне надання певного функціоналу у користування споживачам на обмежений термін	Головний ресурс – люди, даний ресурс - наявний	2-3 місяці
2	Реклама	Залучення власних коштів для реклами товару	1-2 місяці
3	Написання статей та опис товару на відомих ресурсах	Головний ресурс – час, даний ресурс - наявний	2-3 тижні
4	Презентація товару на хакатонах й інших ІТ заходах	Ресурс – час та гроші для участі, наявні	1-3 місяці

4.4. Розроблення ринкової стратегії проєкту

Таблиця 4.15. Вибір цільових груп потенційних споживачів

№	Опис профілю цільової групи потенційних клієнтів	Готовність споживачів сприйняти продукт	Орієнтовний попит в межах цільової групи (сегменту)	Інтенсивність конкуренції в сегменті	Простота входу у сегмент
1	Домовласники /приватні особи	Присутня	Середній	Присутня	Легка
2	Підприємства	Присутня	Середній	Присутня	Складна
Які цільові групи обрано: 1					

Відповідно до проведеного аналізу можна зробити висновок, що розроблюваний продукт призначений для особистого використання фізичними особами в системах розумного будинку будь-якого виду. Відповідно до стратегії охоплення ринку збуту товару обрано стратегії цільового маркетингу та особистого контакту.

Таблиця 4.16. Визначення базової стратегії розвитку

Обрана альтернатива розвитку проєкту	Стратегія охоплення ринку	Ключові конкурентоспроможні позиції відповідно до обраної альтернативи	Базова стратегія розвитку
Надання функціональності що відсутня у товарів-замінників, підтримка клієнтів	Проведення реклами, освітлення унікальної функціональності через інтернет ресурси та інші канали, контакт напряму з споживачами;	Зниження ступеню замінності товару; Прихильність клієнтів; Відмітні властивості товару; Відмітні характеристики товару;	Стратегія диференціації

Таблиця 4.17. Визначення базової стратегії конкурентної поведінки

Чи є проєкт «першопрохідцем» на ринку	Чи буде компанія шукати нових споживачів, або забирати існуючих у конкурентів?	Чи буде компанія копіювати основні характеристики товару конкурента, які?	Стратегія конкурентної поведінки
Ні, оскільки є товари-заміннники, але дані товари замінники не мають деякого необхідного функціоналу	Так, ціль компанії знайти нових споживачів та, частково, забрати існуючих у конкурентів задля задоволення потреб останніх	Компанія частково копіює характеристики товару конкурента, основна ціль компанії розробка нового унікального функціоналу, з підтримкою основного функціоналу конкурентів	Стратегія заняття конкурентної ніші

Таблиця 4.18. Визначення стратегії позиціонування

№	Вимоги до товару цільової аудиторії	Базова стратегія розвитку	Ключові конкурентоспроможні позиції власного стартап-проєкту	Вибір асоціацій, які мають сформувати комплексну позицію власного проєкту
1	Ефективність	Диференціація	Система може бути використана для забезпечення інформаційної безпеки в будь-яких системах розумного будинку	Висока ефективність в оцінюванні загроз інформаційній безпеці
2	Відкритість вихідного коду	Диференціація	Перспектива розвитку проєкту	Розвиток в науці
3	Приватність	Заняття конкурентної ніші	Ваші дані належать тільки вам	Захищеність особистої інформації

Відповідно до проведеного аналізу можна зробити висновок, що стартап-компанія вибирає як базову стратегію розвитку – стратегію диференціації, як базову стратегію конкурентної поведінки – стратегію заняття конкурентної ніші.

4.5 Розроблення маркетингової програми стартап-проєкту

Таблиця 4.19. Визначення ключових переваг концепції потенційного товару

№	Потреба	Вигода, яку пропонує товар	Ключові переваги перед конкурентами (існуючі або такі, що потрібно створити)
1	Функціональність	Можливість налаштування додатку під індивідуальні потреби користувача	Можливість використовувати з будь-якою системою розумного будинку
2	Зручність у використанні	Зрозумілий інтерфейс	Можливість автоматично визначити склад системи та її обмеження

Таблиця 4.20. Опис трьох рівнів моделі товару

<table>
<tr><td>Рівні товару</td><td colspan="3">Сутність та складові</td></tr>
<tr><td>1. Товар за задумом</td><td colspan="3">Система моніторингу та оцінки загроз інформаційній безпеці розумного будинку</td></tr>
<tr><td rowspan="8">2. Товар у реальному виконанні</td><td>Властивості/характеристики</td><td>М/Нм</td><td>Вр/Тх/Тл/Е/Ор</td></tr>
<tr><td>Зручність</td><td>Нм</td><td>Е</td></tr>
<tr><td>Швидкість роботи</td><td>Нм</td><td>Тх</td></tr>
<tr><td>Оптимізація</td><td>Нм</td><td>Тх</td></tr>
<tr><td>Технічна підтримка</td><td>Нм</td><td>Тх</td></tr>
<tr><td>Приватність</td><td>Нм</td><td>Тх</td></tr>
<tr><td colspan="3">Якість: дотримання загальновживаних стандартів, нормативів</td></tr>
<tr><td colspan="3">Пакування: ліцензія на використання системи</td></tr>
<tr><td rowspan="2">3. Товар із підкріпленням</td><td colspan="3">До продажу: наявна повна документація, акції на придбання декількох ліцензій, знижки для певних сегментів на покупку товару</td></tr>
<tr><td colspan="3">Після продажу: додаткова підтримка спеціалістів налаштування, підтримка з боку розробника</td></tr>
<tr><td colspan="4">За рахунок чого потенційний товар буде захищено від копіювання: захист інтелектуальної власності, патент</td></tr>
</table>

Таблиця 4.21. Визначення меж встановлення ціни

Рівень цін на товари-замінники	Рівень цін на товари-аналоги	Рівень доходів цільової групи споживачів	Верхня та нижня межі встановлення ціни на товар/послугу
100-500$	200-1000$	500-5000$/міс	100-200$

Таблиця 4.22. Формування системи збуту

Специфіка закупівельної поведінки цільових клієнтів	Функції збуту, які має виконувати постачальник товару	Глибина каналу збуту	Оптимальна система збуту
Всі користувачі будуть купувати товар поодинці	Можливість скачувати додаток в будь-який час, в будь-якому місці	2 рівня (посередник+клієнт)	Роздріб

Таблиця 4.23. Концепція маркетингових комунікацій

№	Специфіка поведінки цільових клієнтів	Канали комунікацій, якими користуються цільові клієнти	Ключові позиції, обрані для позиціонування	Завдання рекламного повідомлення	Концепція рекламного звернення
1	Домовласники	Інтернет, конференції, приватні зустрічі	Безпека	Показати можливість користування	Рекламне звернення спрямовано до потенційних клієнтів, користування системою

Як результат було створено ринкову (маркетингову) програму, що включає в себе визначення ключових переваг концепції потенційного товару, опис моделі товару, визначення меж встановлення ціни, формування системи збуту та концепцію маркетингових комунікацій.

Висновки по розділу 4

В четвертому розділі описано стратегії та підходи з розроблення стартап-проєкту, визначено наявність попиту, динаміку та рентабельність роботи ринку, як висновок було вказано що існує можливість ринкової комерціалізації проєкту.

Розглянувши потенційні групи клієнтів, бар’єри входження, стан конкуренції та конкурентоспроможність проєкту було встановлено що проєкт є перспективним.

Розглянуто та вибрано альтернативу впровадження стартап-проєкту та доведено доцільність подальшої імплементації проєкту.

ВИСНОВКИ

Проведено аналіз технології "розумний будинок" і існуючих рішень захисту інформації систем розумного будинку показав відсутність єдиної методології опису систем РБ і, отже, відсутність єдиної методології виявлення і оцінки загроз інформаційній безпеці розумного будинку. В результаті аналізу була побудована модель системи інформаційної безпеки для систем РБ і сформований список найбільш ймовірних загроз їх інформаційній безпеці.

Запропоновано класифікацію ймовірних загроз інформаційній безпеці систем розумного будинку, що зв'язує можливі загрози з об'єктами керування системи "розумний будинок". Дана класифікація дозволяє визначати і оцінювати знайдені в системі розумного будинку загрози інформаційній безпеці.

Спроектована система інформаційної безпеки технології розумного будинку, розроблені алгоритми роботи системи, структури опису даних і додаток інформаційної системи. Основні функції системи: визначення складу системи розумного будинку і установка обмежень для показань об'єктів керування користувачем або автоматично, моніторинг даних системи РБ і генерація оповіщень про стан системи РБ. При існуванні в системі розумного будинку невідомої загрози система повідомляє користувача про підозрілі дані.

Розроблена система використана для проведення імітаційних експериментів, в ході яких в системі інформаційної безпеки генерувалися вихідні дані для імітації дій системи розумного будинку, і аналізу виявлення можливих загроз інформаційній безпеці. Результати роботи доводять працездатність розробленого додатку. Даний продукт здійснює моніторинг стану всієї системи і оцінює знайдені загрози.

Таким чином поставлену мету в магістерській дисертації досягнуто а робота носить завершений характер.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. S. Misra, M. Muthucumaru, H. Salman. "System model for the internet of things." Security challenges and approaches in internet of things." Springer, Cham, pp. 5-17, 2017.

2. Test: Smart Home Kits Leave the Door Wide Open – for Everyone [Електронний ресурс]. – URL: https://www.av-test.org/en/news/news-single-view/test-smart-home-kits-leave-the-door-wide-open-for-everyone.

3. Baronti, P., Pillai, P., Chook, V. W. C., Chessa, S., Gotta, A., & Hu, Y. F. (2007). Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee Standards. Computer Communications, 30(7), 1655–1695.

4. Adams, C. E. (2002). Home area network technologies. BT Technology Journal, 20(2), 53–72.

5. Малыш В.Н., Букреев Д.С. Анализ угроз информационной безопасности системы «умный дом» //Труды международного симпозиума «Надежность и качество». 2012. – Т.1.

6. Обзор Bitdefender Box [Електронний ресурс]. – URL: https://www.comss.ru/page.php?id=2397

7. Новое решение Cisco по безопасности следующего поколения (NGFW+NGIPS+AMP) [Електронний ресурс]. – URL: https://habrahabr.ru/company/cisco/blog/237759

8. Kim, G. W., Lee, D. G., Han, J. W., & Kim, S. W. (2007). Security Technologies Based on Home Gateway for Making Smart Home Secure. In Denko, M. (Eds.), Emerging Directions in Embedded and Ubiquitous Computing (pp. 124–135). Springer

9. Ziegler, M., Mueller, W., Schaefer, R., & Loeser, C. (2005). Secure Profile Management in Smart Home Networks. In Proceedings of the 16th International Workshop on Database and Expert Systems Applications. Copenhagen, Denmark

10. D. Crowley, D. Bryan, and J. Savage, “Home invasion 2.0 attacking network-connected embedded devices,” Black Hat USA 2013, Trustwave SpiderLabs and Tabbedout, Tech. Rep., 2013.

11. N. Komninos, E. Philippou and A. Pitsillides, "Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures", IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 1933-1954, 2014.

12. Y. Tanaka, Y. Terashima, M. Kanda and Y. Ohba, A security architecture for communication between smart meters and HAN devices, in IEEE Third Int. Conf. Smart Grid Communications (SmartGridComm), 2012, pp. 460–464.

13. V. Namboodiri, V. Aravinthan, S. N. Mohapatra, B. Karimi and W. Jewell, Toward a secure wireless-based home area network for metering in smart grids, 2014.

14. Снегуров А.В., Ткаченко Е.А., Кравченко А.Д. Риски информационной безопасности систем, построенных по технологии «умный дом» //Восточно-Европейский журнал передовых технологий. 2011. – №3(52) Т.4 2011 – С.30-34.

15. Patton, M.; Gross, E.; Chinn, R.; Forbis, S.; Walker, L.; Hsinchun, C. Uninvited connections: A study of vulnerable devices on the Internet of Things (IoT). In Proceedings of the 2014 IEEE Joint Intelligence and Security Informatics Conference (JISIC), The Hague, The Netherlands, 24–26 September 2014; pp. 232–235.

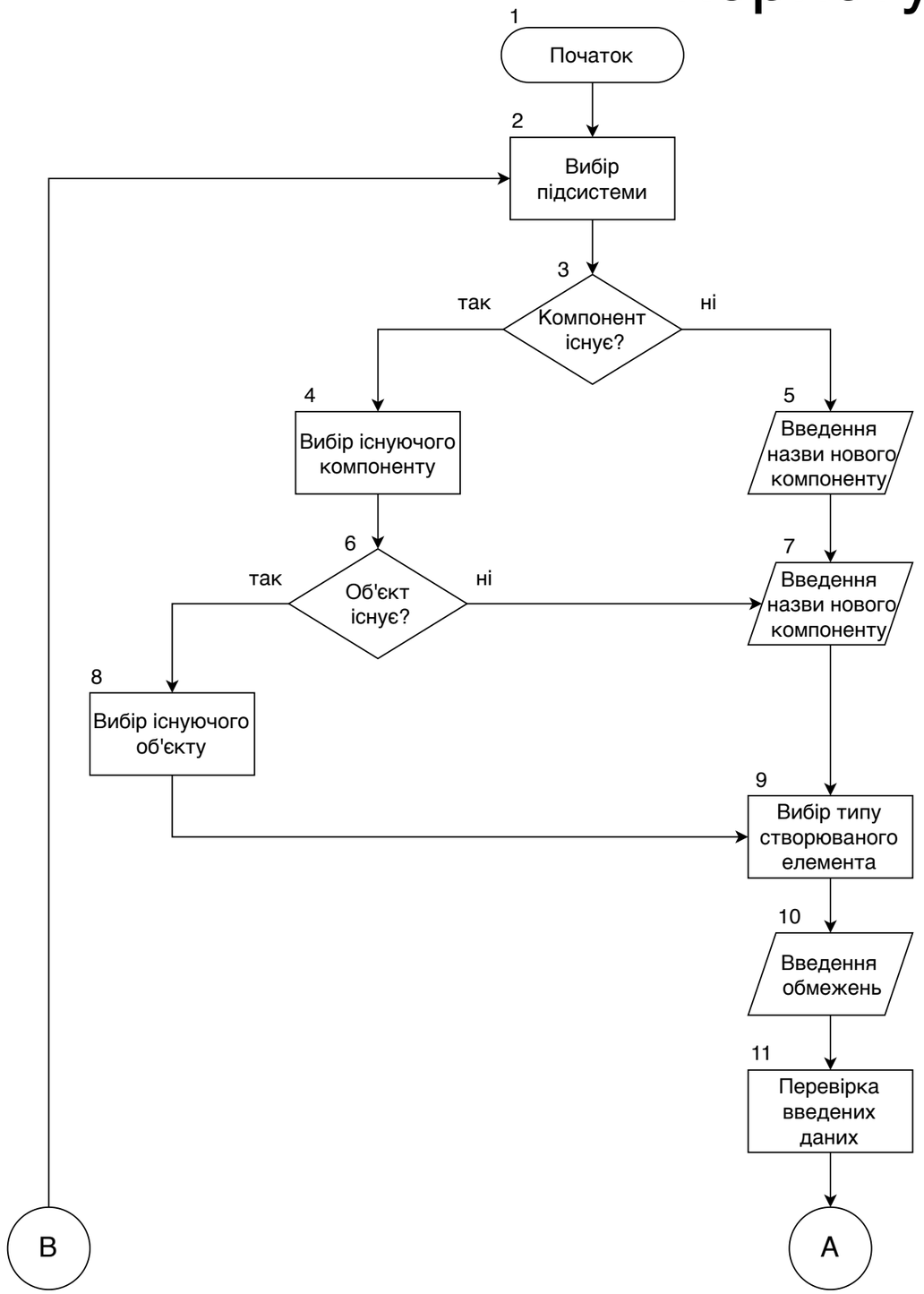
16. Розроблення стартап-проєкту [Електронний ресурс] : Методичні рекомендації до виконання розділу магістерських дисертацій для студентів інженерних спеціальностей / За заг. ред. О.А. Гавриша. – Київ : НТУУ «КПІ», 2016. – 28 с.

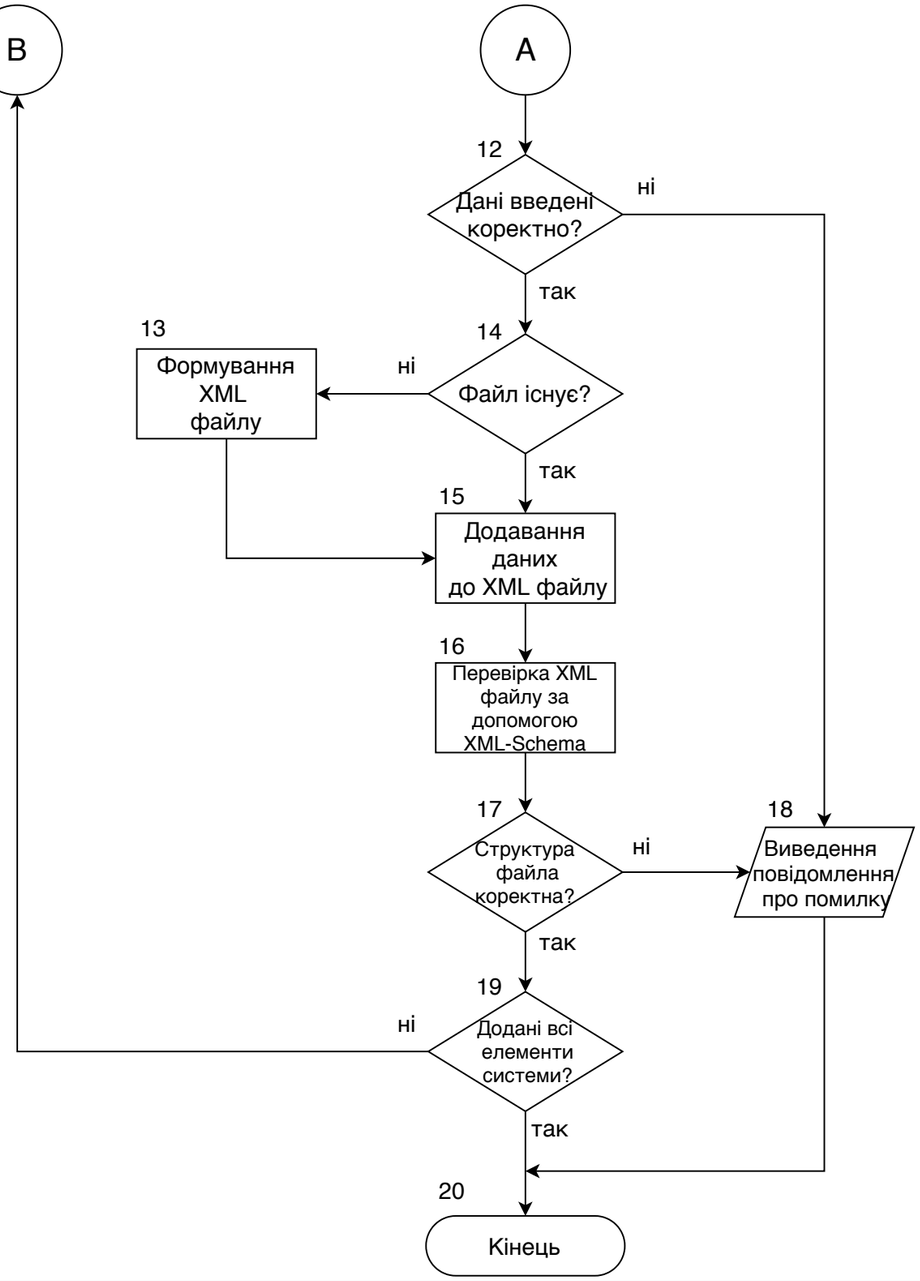
ДОДАТКИ

ДОДАТОК А

Алгоритм визначення складу системи розумного будинку користувачем

Алгоритм визначення складу системи розумного будинку користувачем





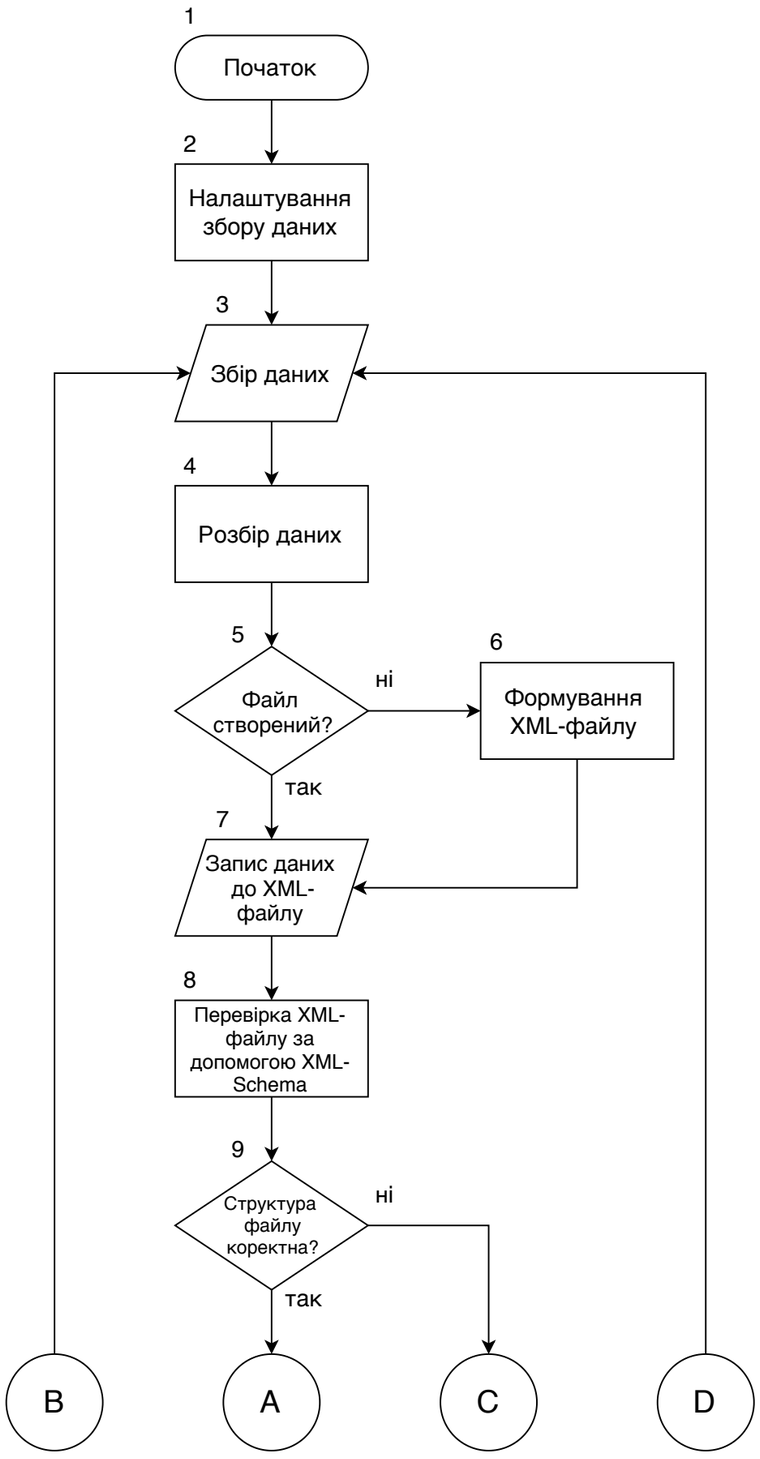
Демонстраційний плакат №1
до магістерської дисертації на тему
"Система моніторингу та оцінки загроз інформаційній безпеці розумного будинку"

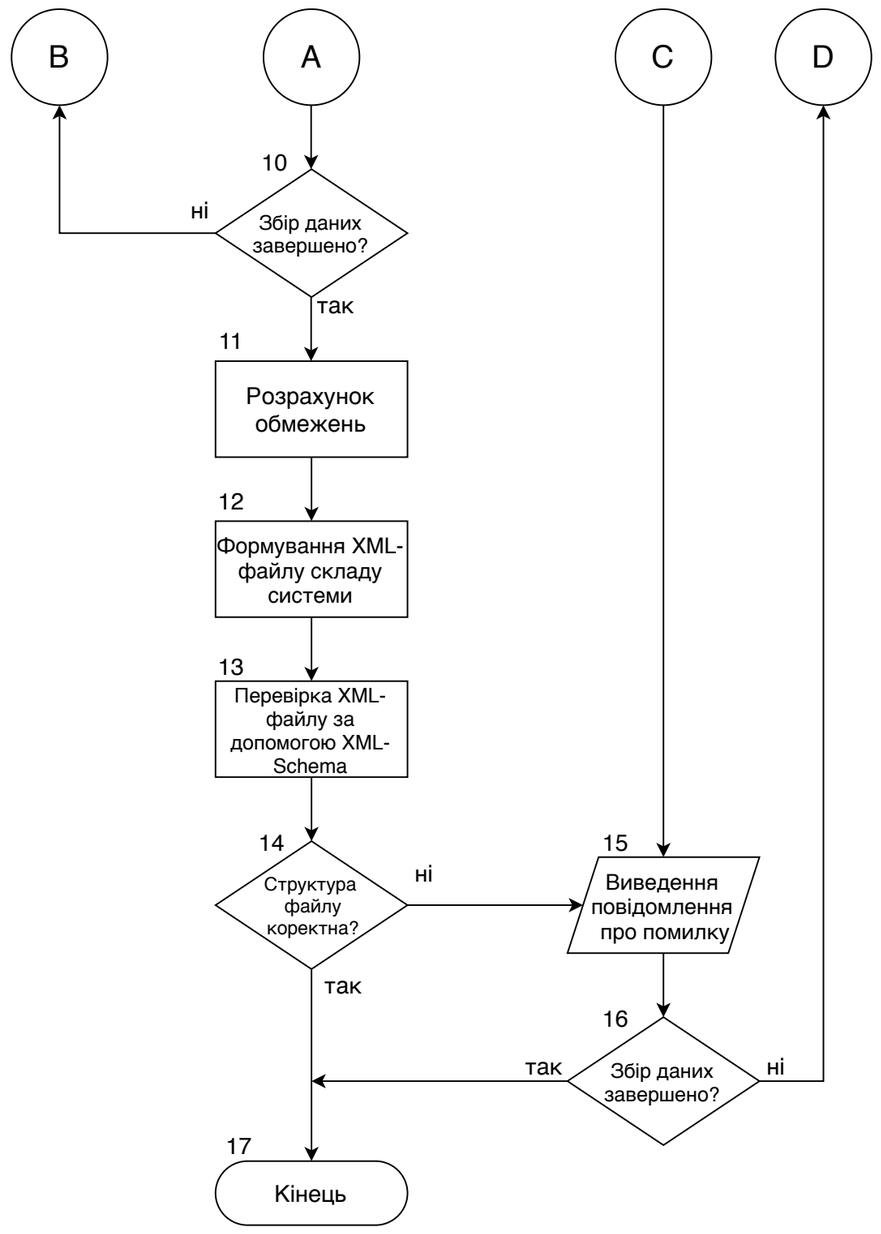
Розробив: Донченко А.Г.
Прийняла: доцент, к.т.н., Цьопа Н.В.

ДОДАТОК Б

Алгоритм автоматичного визначення складу системи розумного будинку

Алгоритм автоматичного визначення складу системи розумного будинку





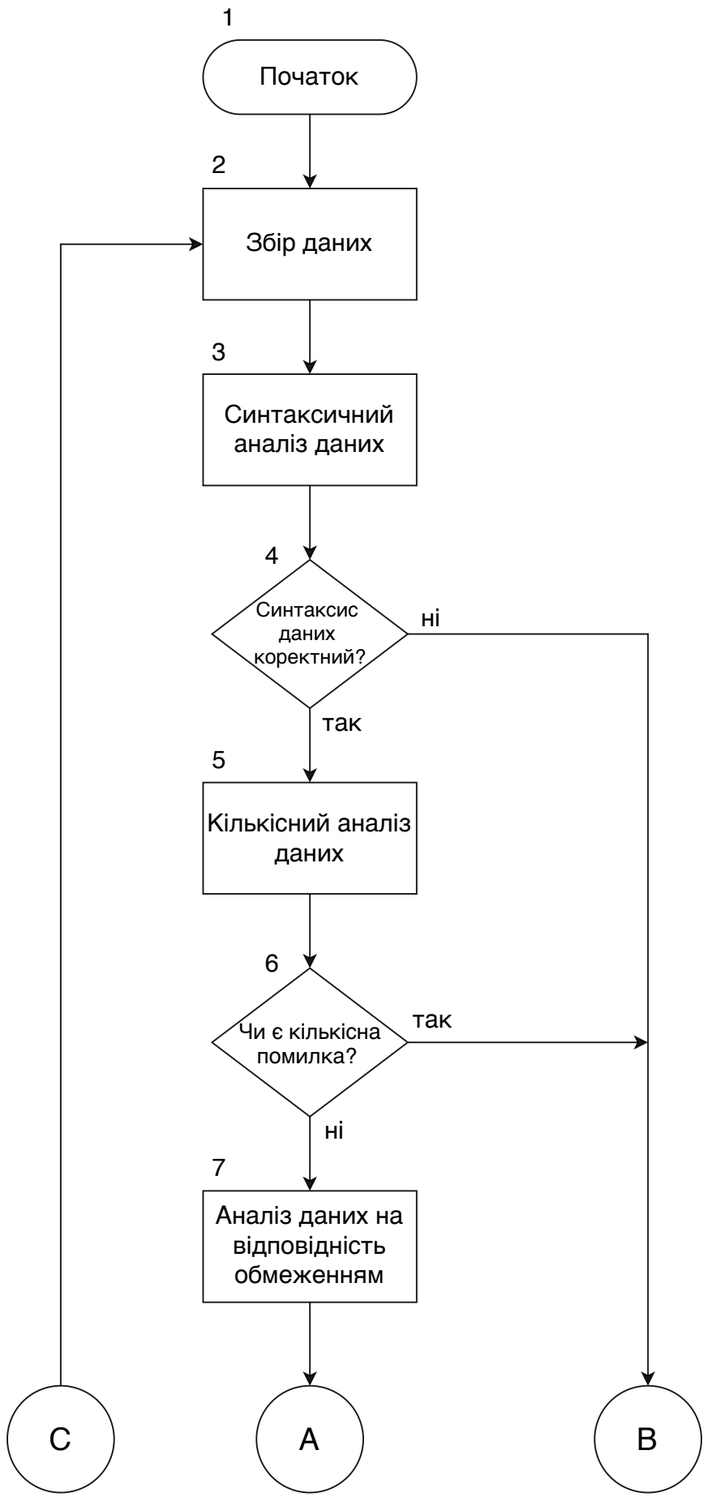
Демонстраційний плакат №2
до магістерської дисертації на тему
"Система моніторингу та оцінки загроз інформаційній безпеці розумного будинку"

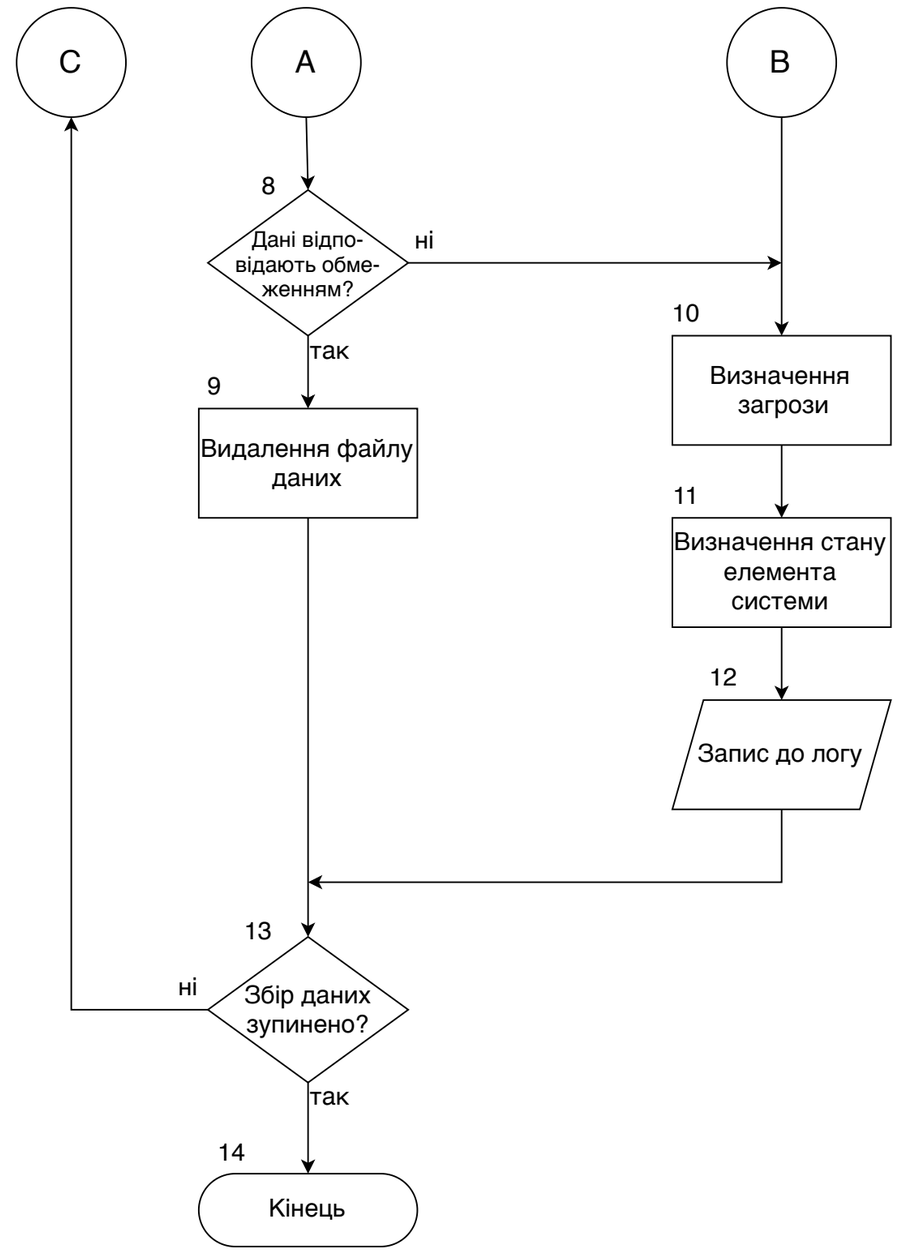
Розробив: Донченко А.Г.
Прийняла: доцент, к.т.н., Цьопа Н.В.

ДОДАТОК В

Алгоритм моніторингу стану системи розумного будинку

Алгоритм моніторингу стану системи розумного будинку





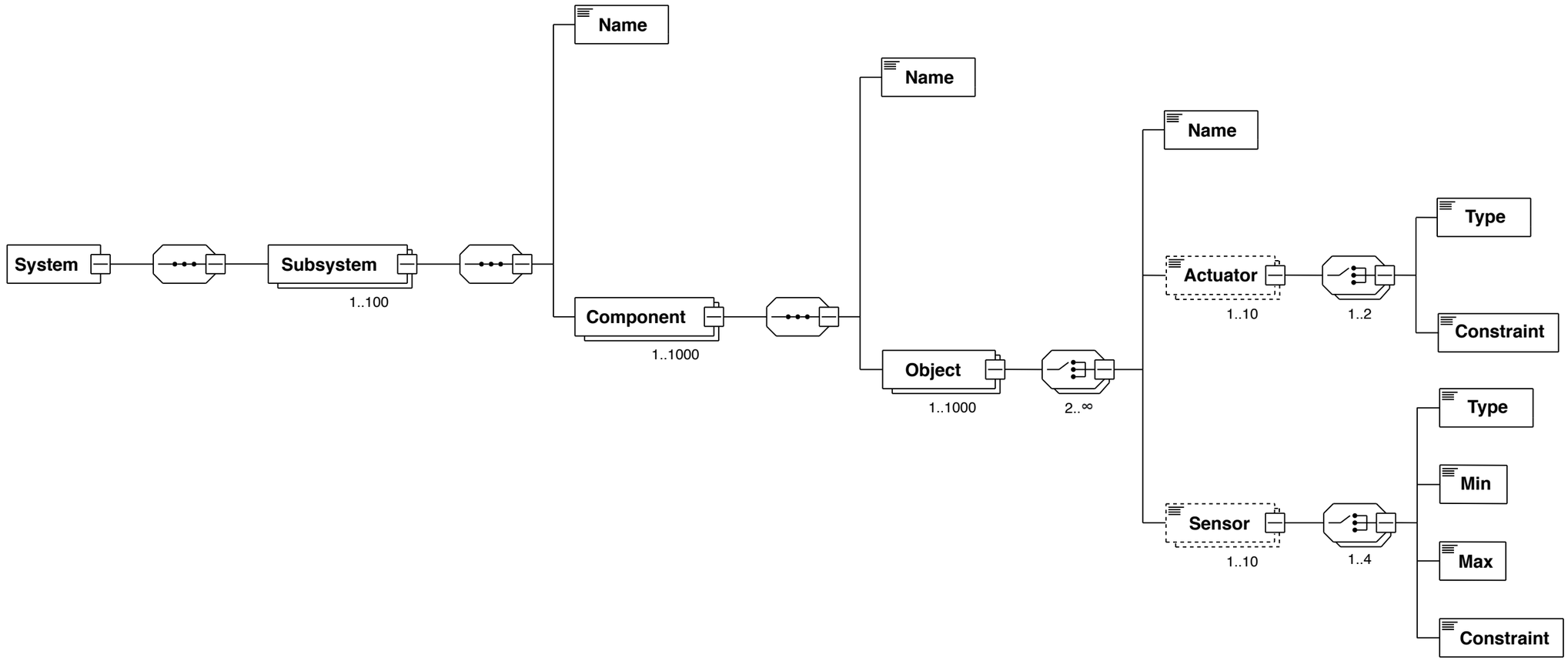
Демонстраційний плакат №3
до магістерської дисертації на тему
"Система моніторингу та оцінки загроз інформаційній безпеці розумного будинку"

Розробив: Донченко А.Г.
Прийняла: доцент, к.т.н., Цьопа Н.В.

ДОДАТОК Г

Схема опису складу системи розумного будинку

Схема опису складу системи розумного будинку



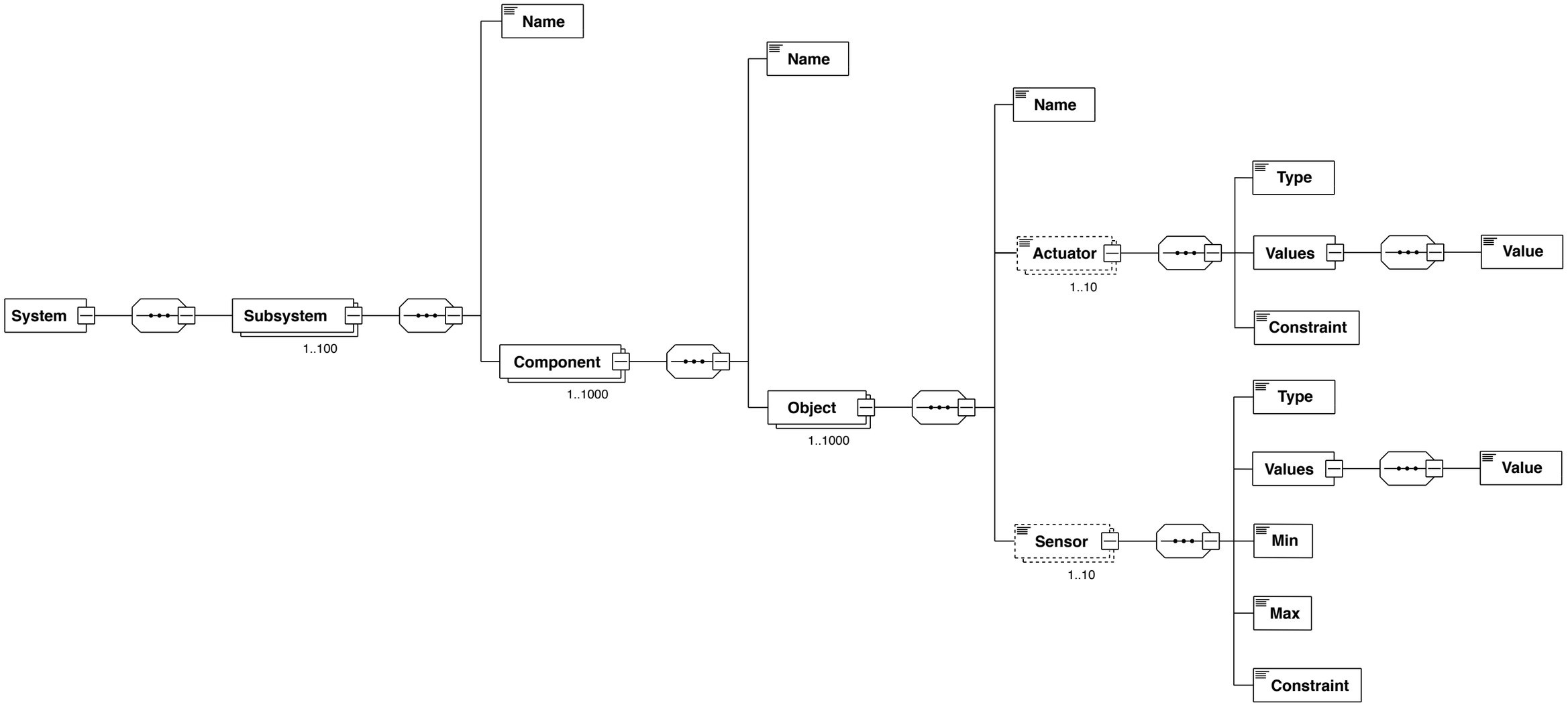
Демонстраційний плакат №4
до магістерської дисертації на тему
"Система моніторингу та оцінки загроз інформаційній безпеці розумного будинку"

Розробив: Донченко А.Г.
Прийняла: доцент, к.т.н., Цьопа Н.В.

ДОДАТОК Ґ

Схема опису автоматично визначеного складу системи розумного будинку

Схема опису автоматично визначеного складу системи розумного будинку



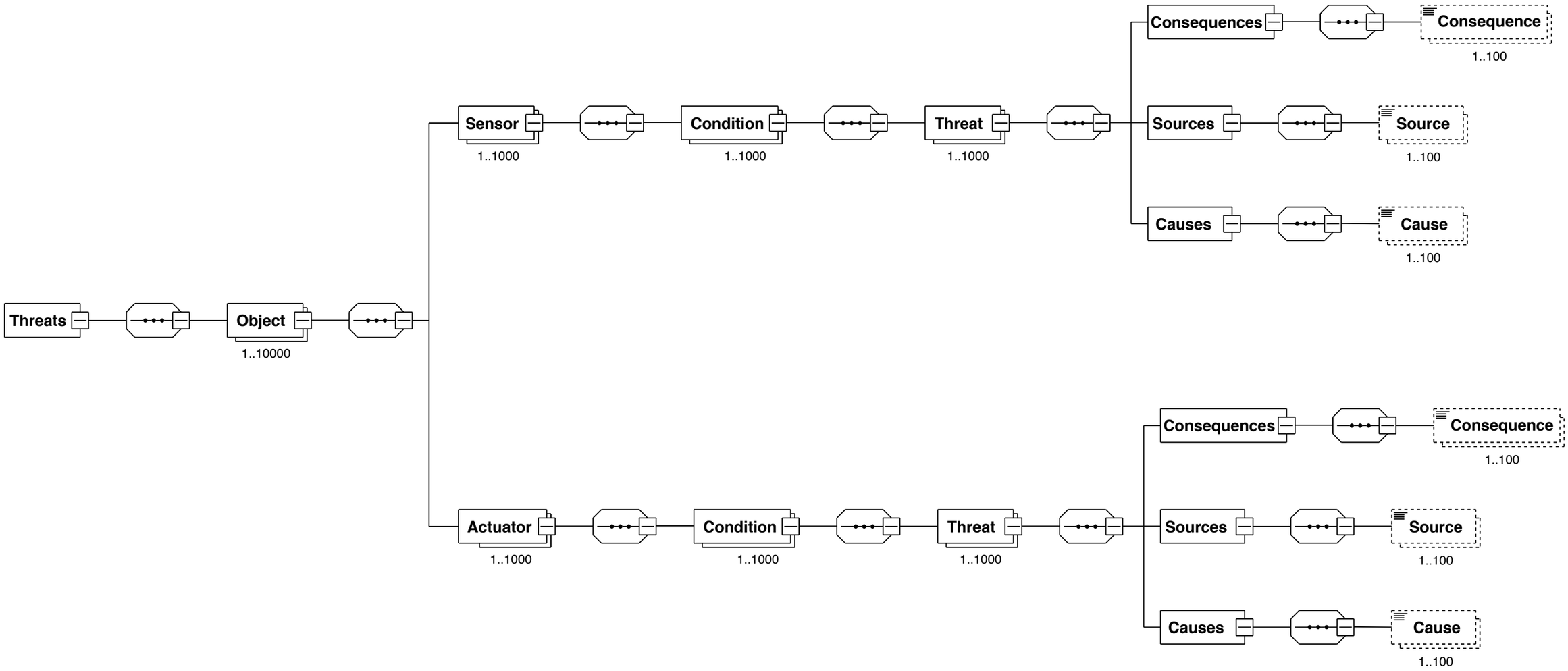
Демонстраційний плакат №5
до магістерської дисертації на тему
"Система моніторингу та оцінки загроз інформаційній безпеці розумного будинку"

Розробив: Донченко А.Г.
Прийняла: доцент, к.т.н., Цьопа Н.В.

ДОДАТОК Д

Схема опису загроз системи розумного будинку

Схема опису загроз системи розумного будинку



Демонстраційний плакат №6
до магістерської дисертації на тему
"Система моніторингу та оцінки загроз інформаційній безпеці розумного будинку"

Розробив: Донченко А.Г.
Прийняла: доцент, к.т.н., Цьопа Н.В.

ДОДАТОК Е

Результат перевірки роботи на співпадіння

UNICHECK

Ім'я користувача:
Лісовиченко Олег Іванович

Дата перевірки:
07.12.2020 20:49:39 EET

Дата звіту:
07.12.2020 20:51:35 EET

ID перевірки:
1005393771

Тип перевірки:
Doc vs Internet + Library

ID користувача:
76913

Назва документа: **Донченко АГ_ІК-91мп**

Кількість сторінок: **35** Кількість слів: **7166** Кількість символів: **54568** Розмір файлу: **93.87 KB** ID файлу: **1005685820**

3.39%
Схожість

Найбільша схожість: **0.56%** з джерелом з Бібліотеки (ID файлу: **5988063**)

0.67% Джерела з Інтернету	11	Сторінка 37
3.01% Джерела з Бібліотеки	52	Сторінка 37

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел